Universidad de Oviedo

Departamento de Matemáticas

Palabras de Engel y anchuras verbales en grupos

Tesis doctoral

Programa de doctorado: Matemáticas

Jorge Martínez Carracedo

Oviedo, 2016

Universidad de Oviedo

Departamento de Matemáticas

Engel words and verbal width in groups

Programa de doctorado: Matemáticas

Jorge Martínez Carracedo

Tesis doctoral, optando a Mención Internacional,
dirigida por **Consuelo Martínez López**

Oviedo, 2016

RESUMEN DEL CONTENIDO DE TESIS DOCTORAL

1.- Título de la Tesis	
Español/Otro Idioma: Palabras de Engel y anchuras verbales en grupos.	Inglés: Engel words and verbal width in groups.

2.- Autor	
Nombre: Jorge Martínez Carracedo	DNI/Pasaporte/NIE: -N
Programa de Doctorado: Matemáticas y Estadística	
Órgano responsable: Departamento de Matemáticas	

RESUMEN (en español)

Dado un grupo arbitrario G y una palabra ω del grupo libre F_r, con r un número natural, se puede considerar la aplicación $\omega_G : G^r \rightarrow G$, que envía cada tupla $(g_1, g_2,...,g_r)$ a su imagen por la palabra ω_G, $\omega_G(g_1, g_2,...,g_r)$. Denotaremos la imagen de esta aplicación por $\omega_G(G)$.

El subgrupo verbal de G asociado a ω se define como el subgrupo generado por $\omega_G(G)$. Se dice que la palabra ω tienen anchura finita en G si existe algún entero m tal que todo producto de ω-valores y sus inversos en G es un producto de a lo sumo m ω-valores y sus inversos en G. El menor entero que cumple dicha propiedad se llama anchura de ω en G.

En primer lugar consideramos la palabra $x^{p\wedge r}y^{p\wedge r}$, con p un número primo y r un número natural mayor que uno. Se consiguió probar que la anchura verbal de estas de palabras sobre los grupos alternados A_n, n≥5, es a lo sumo dos.

Posteriormente consideramos palabras de Engel de longitud m, este es el elemento del grupo libre de rango 2, $E_m(x,y)=[\ldots[x,y],y]\ldots],y]$. En primer lugar conseguimos probar que la anchura verbal de $E_m(x,y)$ sobre los grupos alternados A_n, n≥5, es a lo sumo dos. Es decir, se probó que todo elemento de un grupo alternado A_n, n≥5, se puede escribir como producto de dos palabras de Engel de cualquier longitud.

Además se consiguió probar que en el caso de palabras de Engel de longitud dos, todo elemento del grupo alternado A_n, n≥5, se puede escribir como una palabra de Engel de longitud 2, es decir, la anchura verbal del elemento [[x,y],y] del grupo libre de rango dos es 1 sobre todo grupo A_n, n≥5.

El resultado general de que todo elemento de un grupo alternado A_n, n≥5, es una palabra de Engel de cualquier longitud no se ha conseguido probar. De este modo exploramos un enfoque combinatorio, asociando un grafo a cada elemento σ en A_n, lo que ha permitido probar, computacionalmente, que el resultado se verifica para A_n, 5≤n≤14, lo que no hubiera sido posible de modo directo, tanto por el tamaño de los grupos, como por el hecho de que m, la longitud de la palabra de Engel, no está acotada.

Dada una palabra ω, ¿podemos encontrar una función natural f tal que la anchura

de ω en cualquier grupo finito G esté acotada superiormente por f(d(G)), siendo d(G) el menor tamaño posible de un conjunto generador?

Si dicha función existe, se dice que la palabra ω es elíptica sobre los grupos finitos. Si toda palabra ω es elíptica sobre el grupo G diremos que el grupo es verbalmente elíptico.

Por último se estudió la elipticidad del grupo de Nottingham en característica 0. Dado K un cuerpo de característica 0, este grupo es

$$N_K(t):=\{t+\sum \alpha_k t^{k+1} \mid \alpha_k \in K \text{ para todo } k \in N\},$$

con la composición como operación.

Se probó que $N_K(t)$ es verbalmente elíptico. Para ello se ha trabajado con el álgebra de Lie asociada a la filtración de su serie central descendente.

RESUMEN (en Inglés)

Given an arbitrary group G and a word ω of the free group of Rank r, F_r, with r a natural number, we can consider the function $\omega_G : G^r \rightarrow G$, that maps each tuple $(g_1, g_2,...,g_r)$ to its image by the word ω , $\omega_G(g_1, g_2,...,g_r)$. Let us denote the image of this function by $\omega_G(G)$.

The Verbal Subgroup of G related to ω is defined as the subgroup generated by $\omega_G(G)$. We say that the word ω has finite width in G if there exists an integer m such that every product of ω-values and its inverses in G is a product of, at most, m ω-values and its inverses. The smallest integer for which this property holds is called the Width of ω in G.

First of all, we considered the word $x^{p^r}y^{p^r}$, with p a prime number and r≥1. We proved that the verbal width of this kind of words is at most two over the Alternating groups A_n, n≥5.

Later we considered Engel words of arbitrary length, that is the element of the free group of rank 2 given by $E_m(x,y)=[\ldots[x,y],y]\ldots],y]$. We proved that the verbal width of $E_m(x,y)$ over the Alternating groups A_n, n≥5, is at most two. That is, every element in an Alternating group A_n, n≥5, can be written as a product of, at most, two Engel words of arbitrary length.

We also proved that every element in an Alternating group A_n, n≥5, can be written as an Engel word of length 2.

We have not been able to prove the general result. But we gave a new combinatorial focus. We associate a graph to each element σ in A_n.We can prove, using this graph, that every element in A_n, 5≤n≤14, can be written as an Engel word of arbitrary length.

It is important to emphasize that it would have been impossible to get this result

computationally with a ``brute-force attack". Not only because the high order of A_n when n is big, but also because the length of the Engel word is not bounded.

Given a word ω, can we find a natural function f such that the width of ω in every finite group G is bounded above by f(d(G)), with d(G) the smallest possible order of a generating set?

If that function exists, we say that ω is uniformly elliptic in the set of finite groups. If every word ω is elliptic in a group G, we say that G is verbally elliptic.

We have studied the Nottingham group in Characteristic 0. Given a field in characteristic 0, K, this group is

$$N_K(t):=\{t+\sum \alpha_k t^{k+1} \mid \alpha_k \in K \text{ para todo } k \in N\}$$

We have proved that $N_K(t)$ is verbally elliptic. For that, we have worked with the Lie algebra associated to the lower central series of the group $N_K(t)$.

SR. DIRECTOR DE DEPARTAMENTO DE MATEMÁTICAS.
SR. PRESIDENTE DE LA COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO EN MATEMÁTICAS Y ESTADÍSTICA.

Esta investigación ha sido parcialmente financiada por los proyectos del Ministerio de Economía y Competitividad MTM2010-18370-C04-01 y MTM2013-45588-C3-1-P, y por el proyecto GRUPIN14-142 de la Fundación para el Fomento en Asturias de la Investigación Científica Aplicada y la Tecnología (FICyT) del Principado de Asturias.

This research was partially supported by projects MTM2010-18370-C04-01 and MTM2013-45588-C3-1-P of Spanish Ministry of Economy and Competitiveness and GRUPIN14-142 of FICyT, Principado de Asturias.

Agradecimientos

En primer lugar, querría expresar mi agradecimiento a mi directora de Tesis, la profesora Consuelo Martínez López, por su tiempo, su esfuerzo y por haberme dado esta oportunidad. Este trabajo no hubiera sido posible de no ser por ella.

Me gustaría dar las gracias en segundo lugar al Profesor Efim Zelmanov por recibirme en la Universidad de California (San Diego), por su ayuda y por supervisar y dirigir mi trabajo durante las dos estancias que realicé en su Universidad.

Desearía agradecer también al Profesor Santos González Jiménez su confianza y ánimos durante el desarrollo de este trabajo.

Me gustaría mencionar y agradecer igualmente la ayuda recibida de todos los miembros del grupo de Álgebra, Codificación y Criptografía de la Universidad de Oviedo. Entre ellos, Adriana Suárez Corona, Cristina García Pillado, Hugo Villafañe Roca e Ignacio Fernández Rúa.

También me gustaría agradecer al Ministerio Economía y Competitividad la concesión de una beca-contrato de Formación del Personal Investigador (FPI) y al Gobierno del Principado de Asturias por la concesión de un contrato de Investigación que me permitieron obtener la financiación necesaria para poder llevar a cabo este trabajo.

Por último, gracias a todos mis familiares y amigos por el apoyo y los ánimos que he recibido de su parte durante estos años.

Acknowledgments

First of all, I want to express my gratitude to my PhD. advisor, Professor Consuelo Martínez López, in appreciation for her effort and the opportunity she has given to me. This work would not be possible without her help.

Secondly, I would also like to show my gratitude to Professor Efim Zelmanov, for receiving me at the University of California (San Diego), for his help and for supervising and directing my work during my two research stays.

I would like to thank Professor Santos González Jiménez his trust and encouragement during the development of this research.

I want to mention and show my gratitude for all the help provided, to all the members of the group of Algebra, Codification and Cryptography of the University of Oviedo. Among them, Adriana Suarez Corona, Cristina García Pillado, Hugo Villafañe Roca and Ignacio Fernandez Rúa.

As well, I would like to thank the Ministry of Economy, for the scholarship award (FPI), and the government of the Principality of Asturias for the research contract award. Both of them allowed me to get the necessary funding to carry through with this work.

Finally, to all my family and friends, thank you for your support and encouragement during these years.

Índice general

Introducción

El Problema de Waring es un famoso problema en teoría de números que fue enunciado por Edward Waring en 1770: Existe una función $g : \mathbb{N} \to \mathbb{N}$ verificando que todo número natural se puede escribir como suma de no más de $g(k)$ potencias k-ésimas. Waring no dio su demostración.

Fue Hilbert quién, en 1909, lo demostró, conociéndose desde entonces como Teorema de Waring-Hilbert. Se puede encontrar una versión simplificada de la demostración de Hilbert en [4], dónde se presenta una fórmula precisa para la función $g(k)$.

Recientemente se ha suscitado gran interés en resultados análogos al anterior dentro de la Teoría de Grupos. En este ámbito, el nuevo objetivo se centra en conocer cuando es posible expresar todos los elementos de un grupo como producto de ciertos elementos especiales de dicho grupo, por ejemplo, como producto de elementos de una clase de conjugación o potencias de elementos. En general, elementos que son valores de una palabra ω del grupo libre $\mathcal{F}_r$, con r un número natural.

En general, dado un grupo arbitrario G y una palabra $\omega \in \mathcal{F}_r$, con r un número natural, se puede considerar la aplicación $\omega_G : G^r \to G$, que envia cada tupla $(g_1, g_2, ..., g_r)$ a su imagen por la palabra ω, $\omega_G(g_1, g_2, ..., g_r)$. Denotaremos la imagen de esta aplicación por $\omega_G(G)$.

El subgrupo verbal de G asociado a ω se define como el subgrupo generado por $\omega_G(G)$. Se dice que la palabra ω tienen anchura finita en G si existe algún entero $m \in \mathbb{N}$ tal que todo producto de ω-valores y sus inversos en G es un producto de a lo sumo m ω-valores y sus inversos en G. El menor entero que cumple dicha propiedad se llama anchura de ω en G.

Desde mediados del siglo XX se han planteado preguntas del siguiente tipo: Dada una palabra ω, ¿podemos encontrar una función natural f tal que la anchura de ω en cualquier grupo finito G esté acotada superiormente por $f(d(G))$, siendo $d(G)$ el menor tamaño posible de un conjunto generador?

Si dicha función existe, se dice que la palabra ω es elíptica sobre los grupos

finitos. Si toda palabra ω es elíptica sobre el grupo G diremos que el grupo es verbalmente elíptico.

Como se puede observar, hay una cierta similitud entre esta última pregunta y el Problema de Waring, por lo que podemos interpretar que se trata de buscar análogos a dicho resultado en contextos no conmutativos.

Se han realizado numerosas contribuciones desde que se iniciara el estudio de los subgrupos verbales. En [29] se prueba que toda palabra ω tiene anchura finita en un grupo finito G. Más aun, se sabe que la anchura verbal de ω sobre G estará acotada superiormente por $\mid G \mid$. De esta manera la pregunta sobre si los grupos finitos son ω-elípticos queda contestada afirmativamente.

También se tienen resultados sobre la anchura verbal en grupos infinitos. Uno de los primeros fue probado por Romankov (véase [25]) quién probó que todo grupo finitamente generado y virtualmente-nilpotente es verbalmente elíptico.

Si definimos rango (de Prüfer) de un grupo G como

$$rk(G) := sup\{d(H) \mid H \quad \text{es un subgrupo finitamente generado de } G\},$$

se puede deducir un resultado algo más general (ver [29]) a partir del teorema de Romankov: Todo grupo virtualmente nilpotente y de rango finito es verbalmente elíptico. En estos dos resultados se estudia por primera vez la anchura verbal en grupos infinitos.

Cabe preguntarse si existe alguna palabra (no trivial) que posea anchura finita en todo grupo G. La respuesta a esta pregunta se debe a Akbar Rhemtulla, quien prueba en [24] que una palabra ω del grupo libre $\mathcal{F}_k$ tiene anchura finita sobre todo grupo G si y sólo si existen enteros $e_1, ..., e_k$ tales que $mcd(e_1, ..., e_k) = 1$ y

$$\omega \in x_1^{e_1} ... x_k^{e_k} \mathcal{F}_k'.$$

En 1951, Oystein Ore probó en [23] que todo elemento de un grupo Alternado simple A_n, $n \geq 5$, se puede escribir como el conmutador de dos elementos del grupo.

El resultado de Ore dice que la palabra $\tau := x_1^{-1} x_2^{-1} x_1 x_2$, del grupo libre de rango 2, $\mathcal{F}_2$, cumple que $\tau(A_n) = A_n$ para todo $n \geq 5$. Conjeturó (*Conjetura de Ore*) que para todo grupo simple finito G, se tiene que $\tau(G) = G$. En particular, la conjetura de Ore plantea que la palabra τ es elíptica sobre los grupos simples finitos.

Un primer avance en la conjetura de Ore se debe a Wilson, que prueba en [32] que existe una constante k tal que $\tau(G)^k = G$, para todo grupo simple finito G.

Las técnicas utilizadas para probar el resultado se basan en lógica de primer orden, ultraproductos y la clasificación de los grupos simples finitos.

También existen resultados relativos a la palabra $\xi := x^n$, con n un número natural. En 1996, Martínez y Zelmanov [22] y en 1997, Salx and Wilson [27], probaron independientemente, que para todo grupo simple finito suficientemente grande se puede encontrar una constante k para la cual se verifica que

$$\underbrace{\xi(G)...\xi(G)}_{k} = G.$$

Es decir, todo elemento de un grupo simple finito suficientemente grande, G, se puede expresar como producto de $g(n)$ potencias n-ésimas, para una cierta función natural g, o equivalentemente, la palabra $\xi = x^n$ es elíptica sobre grupos simples finitos suficientemente grandes.

En el Capítulo 1 de este trabajo, probaremos que para los grupos alternados y $n = p^k$, con p un número primo, podemos tomar como función $g(n)$ la función constante 2.

Un avance importante en la conjetura de Ore se produjo en 2001, cuando Liebeck y Shalev [18] probaron que para toda palabra $\omega \neq 1$ existe un entero positivo $N = N(\omega)$ tal que para todo grupo simple finito G, con $|G| \geq N(\omega)$, se tiene que

$$\omega(G)^3 = G.$$

En 2008, Larsen y Shalev [15] extendieron el resultado anterior probando que para ciertas familias de grupos simples finitos, se puede reemplazar el exponente 3 por 2.

Finalmente, en 2010, M.W. Liebeck, E.A. O'Brien, A. Shalev y P.H. Tiep [16] demostraron la Conjetura de Ore, probando que para todo grupo simple finito G, se tiene que $G = \tau(G)$, con $\tau := x_1^{-1}x_2^{-1}x_1x_2$ el conmutador.

Las técnicas usadas para la demostración de este resultado son muy elaboradas y combinan tres elementos principalmente: teoría de caracteres, inducción sobre la dimensión y cálculos computacionales. El lenguaje de programación usado durante dicha prueba fue MAGMA, con el que se consiguió construir la tabla de caracteres para numerosos casos que permitirían posteriormente usar argumentos inductivos.

Uno de los pilares de la demostración es un conocido resultado de Frobenius ([5]) que prueba que un elemento g de un grupo finito G es un conmutador si y sólo si

$$\sum_{\chi \in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Una vez probada la Conjetura de Ore, parece natural preguntarse sobre

el comportamiento de una palabra de Engel de longitud arbitraria,

$$E_m = [...[x, \overbrace{y], y], ..., y}^{m}],$$

con m un número natural. ¿Podemos afirmar que todo grupo simple finito G verifica que $G = E_m(G)$?.

Nuestro primer objetivo era probar el resultado mencionado para los grupos alternados A_n, $n \geq 5$. En el Capítulo 2 veremos que todo elemento de dichos grupos se puede escribir como producto de, a lo sumo, dos palabras de Engel de longitud arbitraria. Es decir, probaremos que para cualesquiera números naturales n y m se tiene que

$$A_n = E_m(A_n)E_m(A_n).$$

En el capítulo 3 estudiaremos palabras de Engel de longitud 2, $E_2(x, y) = [[x, y], y]$, y probaremos que todo elemento de un grupo Alternado A_n, $n \geq 5$, se puede escribir como una palabra de Engel de longitud 2 en A_n. Es decir,

$$A_n = E_2(A_n) \quad \text{para todo} \quad n \geq 5.$$

Queremos destacar que las técnicas utilizadas en la demostración de estos resultados son técnicas elementales de teoría de grupos, a diferencia de lo que ocurre en la mayoría de artículos citados, en los que se usan técnicas avanzadas de Teoría de Grupos, Teoría de Caracteres o Teoría Analítica de Números.

Notemos también que el resultado obtenido en el Capítulo 2 no es un caso particular del probado por Larsen y Shalev [15] para grupos alternados, dado que en el citado artículo se prueba el resultado para órdenes suficientemente grandes.

El resultado general de que todo elemento de un grupo alternado A_n, $n \geq 5$, es una palabra de Engel de cualquier longitud no se ha podido probar. En el Capítulo 4 exploramos un enfoque combinatorio asociando un grafo a cada elemento $\sigma \in A_n$, lo que ha permitido probar, computacionalmente, que el resultado se verifica para A_n, $5 \leq n \leq 14$, lo que no hubiera sido posible de modo directo, tanto por el tamaño de los grupos, como por el hecho de que m, la longitud de la palabra de Engel, no está acotada.

En el último capítulo de este trabajo se estudiará el grupo de Nottingham en característica 0. Dado $\mathbb{K}$ un cuerpo de característica 0, este grupo es

$$N_{\mathbb{K}}(t) := \{t + \sum_{k \geq 1} \alpha_k t^{k+1} \mid \alpha_k \in \mathbb{K} \quad \forall k \in \mathbb{N}\},$$

con la composición como operación.

Probaremos que $N_{\mathbb{K}}(t)$ es verbalmente elíptico. Trabajaremos también con el álgebra de Lie asociada a la filtración de su serie central descendente y la relacionaremos con el álgebra de Virasoro y algunas de sus subálgebras.

Introduction

Waring's Problem, proposed by Edward Waring in 1770, is a famous problem in Number Theory. Waring enunciated it, without proof, as indicated below: there exists a function $g : \mathbb{N} \to \mathbb{N}$ verifying that every natural number can be written as the sum of no more than $g(k)$ k-th powers.

Hilbert was who, in 1909, gave the proof of Waring's Problem, that, since then, is known as Waring-Hilbert's Theorem. A simplified version of Hilbert's proof can be found in [4], together with an accurate formula for the function $g(k)$.

Recently one can observe a growing interest in similar results inside Group Theory. In this context, the aim focuses on the possibility of exposing all elements of a group as a product of particular elements, for instance, elements of a conjugacy class or power of elements. In general, this can be formulated using the free group $\mathcal{F}_r$, with r a natural number.

Given an arbitrary group G and a word $\omega \in \mathcal{F}_r$, with r a natural number, we can consider the function $\omega_G : G^r \to G$, that maps each tuple $(g_1, g_2, ..., g_r)$ to its image by the word ω, $\omega(g_1, g_2, ..., g_r)$. Let us denote the image of this function by $\omega(G)$.

The Verbal Subgroup of G related to ω is defined as the subgroup generated by $\omega_G(G)$. We say that the word ω has finite width in G if there exists an integer $m \in \mathbb{N}$ such that every product of ω-values and its inverses in G is a product of, at most, m ω-values and its inverses. The smallest integer for which this property holds is called the Width of ω in G.

Since the mid-twentieth century, questions of the following type have been formulated: Given a word ω, can we find a natural function f such that the width of ω in every finite group G is bounded above by $f(d(G))$, with $d(G)$ the smallest possible order of a generating set?

If that function exists, we say that ω is uniformly elliptic in the set of finite groups. If every word ω is elliptic in a group G, we say that G is verbally elliptic.

We can see some similarities between the last question and Waring's Problem , so we can understand the last mentioned problem as a kind of analogue to Waring's Problem in a non-commutative context.

Numerous contributions have been made since the study of verbal subgroups began. In [29], it is proved that every word ω has finite width in a finite group G. Even more, the verbal width of ω in G is bounded above by $\mid G \mid$. In this way, we have an affirmative answer to the question: Are finite groups ω-elliptic?

There are also some results about verbal width in infinite groups. One of the first was proved by Romankov (see [25]). He proved that every finitely generated and virtually-nilpotent group is verbally elliptic.

The term rank that we are going to use is the Prüfer rank; that is

$$rk(G) := sup\{d(H) \mid H \quad \text{is a finitely generated subgroup of } G\}.$$

It is possible to give a stronger result (see [29]) from Romankov Theorem: Every virtually-nilpotent group with finite rank is verbally elliptic. These two results are the first ones that studied the verbal width in infinite groups.

We can ask if there exists a word (non trivial) with finite width in every group G. The answer to this question was given by Akbar Rhemtulla, who proved in [24] that any word ω of the free group $\mathcal{F}_k$ has finite width in every group G if and only if there exist integers $e_1, ..., e_k$ such that $gcd(e_1, ..., e_k) = 1$ and

$$\omega \in x_1^{e_1}...x_k^{e_k}\mathcal{F}_k'.$$

In 1951, Oysten Ore published (see [23]) a result proving that every element of an alternating simple group can be written as a commutator of elements in the same alternating group.

Notice that Ore's result says that if we take the word $\tau := x_1^{-1}x_2^{-1}x_1x_2$ inside the free group of rank 2, $\mathcal{F}_2$, then $\tau(A_n) = A_n$, for all $n \geq 5$. Moreover, he conjectured that the result is also true for an arbitrary simple finite group, that is, $\tau(G) = G$ (The Ore Abstract Conjecture). In particular, the Ore Conjecture asks if the word τ is elliptic in every finite simple group.

In 1994, Wilson [32], makes progress on the Ore Conjecture. He proves that if we take $\tau := x_1^{-1}x_2^{-1}x_1x_2$ and a finite simple group G, then there exists a constant k such that, $\tau(G)^k = G$.

The techniques used to prove this result are based on first order logic propositions, ultraproducts and the classification of finite simple groups.

On the other hand, there are some results about the word $\xi := x^n$, with n a natural number. In 1996, Martínez and Zelmanov [22] and in 1997, Saxl and Wilson [27], proved, independently, that for every finite simple group big enough, there exists a constant k such that $\xi(G)^k = G$. From these results

it follows that every element of a simple, finite, big enough group G, can be expressed as the product of $g(n)$ n-th powers, for a natural function g, or equivalently, the word $\xi = x^n$ is elliptic in every finite simple group big enough.

In Chapter 1, we will prove that for Alternating groups and $n = p^k$, with p a prime number, the function $g(n)$ is at most 2.

In 2001 Liebeck and Shalev [18] achieved important progress in The Ore Conjecture when they proved that for every word $\omega \neq 1$ there exists a positive integer $N = N(\omega)$ such that for every finite simple group G, with $|G| \geq N(\omega)$ we have

$$\omega(G)^3 = G.$$

In 2008, Larsen and Shalev [15] improved the previous result proving that the exponent 3 can be replaced by 2 in certain families of finite simple groups.

Finally, in 2010, M.W. Liebeck, E.A. O'Brien, A. Shalev and P.H. Tiep [16] finished the proof of The Ore Conjecture. They proved that for every finite simple group G, $G = \tau(G)$, where $\tau := x_1^{-1}x_2^{-1}x_1x_2$. The techniques used for these results are very elaborate and mainly combine three elements: Character Theory, Induction assumptions and computations using algebraic computer programs.

A known result of Frobenius [5] plays an important role in the proof: An element g of a finite group G is a commutator if and only if

$$\sum_{\chi \in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Once the Ore Conjecture has been proved, it seems natural to consider Engel words of arbitrary length,

$$E_m = [...[x, \overbrace{y], y], ..., y}^{m}],$$

with n a natural number, and ask if it is still true that $G = E_n(G)$ for every finite simple group G .

Our first aim was to prove the above result for alternating simple groups A_n, $n \geq 5$. In Chapter 2, we will prove that every element of those groups can be written as the product of at most two Engel words of arbitrary length, that is, for every natural numbers n and m we have

$$A_n = E_m(A_n)E_m(A_n).$$

In Chapter 3 we will study Engel words of length 2, $E_2(x, y) = [[x, y], y]$. We will prove that every element in an Alternating group A_n, $n \geq 5$, can be

written as an Engel word of length 2 in A_n; that is

$$A_n = E_2(A_n) \quad \text{para todo} \quad n \geq 5.$$

Let's remark that we will use only elementary techniques of Group Theory in these results, unlike what happens in previous works, in which highly sophisticated techniques were used.

Notice that the result that we have got in Chapter 2 is not a particular case of the one proved by Larsen and Shalev [15] for alternating groups, since their result is proved for big enough orders.

We have not been able to prove the general result. But in chapter 4, we show a new combinatorial approach. We associate a graph to each element $\sigma \in A_n$. We can prove, using this graph, that the result is true for A_n, $5 \leq n \leq 14$.

It is important to emphasize that it would have been impossible to get this result computationally with a "brute-force attack". Not only because the high order of A_n when n is big, but also because the length of the Engel word is not bounded.

In the last Chapter of this work we will study the Nottingham group in Characteristic 0. Given a field in characteristic 0, $\mathbb{K}$, this group is

$$N_{\mathbb{K}}(t) := \{t + \sum_{k \geq 1} \alpha_k t^{k+1} \mid \alpha_k \in \mathbb{K} \quad \forall k \in \mathbb{N}\}.$$

We will prove that $N_{\mathbb{K}}(t)$ is verbally elliptic. For that, we will work with the Lie algebra associated to the lower central series of the group $N_{\mathbb{K}}(t)$.

Capítulo 1

Powers in Alternating Simple Groups

In any group G, G^d the subgroup generated by d-th powers of elements in G and G' are normal subgroups. So, if G is a finite non-abelian simple group it is clear that $G = G'$ and if d is not divisible by $exp(G)$, then $G = G^d$. So, every element of G can be expressed both as a product of a finite number of commutators in G and as a product of finitely many d-th powers in G. But the existence of a bound for the number of factors in any element of G has important consequences, for instance in profinite groups.

In 1996, C. Martínez and E. Zelmanov [22] proved that for a natural number $d \geq 1$, there exists a function $N(d)$ such that for an arbitrary simple group G either $G^d = 1$ or $G = \{a_1^d ... a_N^d \mid a_i \in G\}$.

In particular, for alternating groups A_n, $n \geq 5$, Martínez and Zelmanov used a result by Bertran that says that any even permutation in A_n can be written as a product of two cycles, each one of length l, if and only if, $[3n/4] \leq l \leq n$..

Clearly, it seems that the bound depends on d. For instance, if $d = 2$ every element in A_n, $n \geq 5$, is a product of two squares in A_n. However, if $d = 210$, it is impossible to write every 7-cycle in A_7 as a product of two 210-th powers in A_7. But, for every natural number $m' < 210$, it can be proved that every element in A_7 can be written as a product of two m'-th powers.

Still, it is natural to ask if we can find a general constant N such that every element in an alternating group A_n, $n \geq 5$, can be written as a product of N d-th powers of elements in A_n. In this paper it is proved that this is the case for $d = p^r$, where p is a prime number and r is a natural number. And in this case, $N = 2$.

These ideas can be reformulated in an slightly different way. Given an arbitrary group G and a word in the free group of rank r, $\omega \in \mathbb{F}_r$, with r a

natural number, we can consider the word map $\omega : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$ that maps each tuple $(g_1, g_2, ..., g_r)$ to $\omega(g_1, g_2, ..., g_r)$. It has sense to ask if this word map is surjective.

Of course, there are words for which $\omega(G) \neq G$. For example, the word x^2 is not surjective on any finite non abelian simple group. Nevertheless, some word maps are surjective, and it is an interesting problem in Group Theory to determine which ones are.

The first non-trivial example of a word map which is surjective on all finite non-abelian simple groups is the commutator map $[x, y]$. It was proved in [16], giving a positive answer to a conjecture formulated by Ore, who had proved in 1951 [23] the result for alternating groups.

In [19] authors proved in the same article that every element of a sufficiently large finite simple group is a product of two squares and posed the conjecture that the word x^2y^2 is surjective . This conjecture was proved in [17], where authors also proved that if $p > 7$ is a prime number, then any element of a finite non-abelian simple group G is a product of two p-th powers.

At the same time, R. Guralnick and G. Mall got a new proof using some results about conjugacy classes. In [6], they proved that there always exist two conjugacy classes in a finite non abelian simple group such that every non trivial element of the group belongs to the product of these conjugacy classes. This result is used to prove that every element in a finite non abelian simple group can be written as a product of two p^k-th powers, with p a prime number.

We must emphasize that the proof of all these results is highly nontrivial. Our aim here is to show a proof of the mentioned result for alternating groups A_n, $n \geq 5$, that uses only elementary techniques.

Let's mention an elementary fact that will be extensively used in what follows. Given a group G and a natural number $n \geq 1$, the mapping

$$\begin{aligned} \varphi_n : G &\longrightarrow G \\ g &\mapsto g^n \end{aligned}$$

is bijective if an only if the greatest common divisor $gcd(n, exp(G)) = 1$.

Indeed, if we take a prime divisor p of $exp(G)$ and n, there exists an element in $g \in G$ of order p. So $\varphi(g) = \varphi(1) = 1$.

The next elementary result will very useful in chapter.

Theorem 1.0.1. *If G is a finite group, g is an element of G and $d \geq 1$ is an integer such that $gcd(o(g), d) = 1$, then $g = (g^s)^d$ for some integer $s \geq 1$.*

Proof. It suffices to consider the cyclic group $\langle g \rangle$. As the $gcd(o(g), d) = 1$, we can apply the Bezout's Identity to get that there exist $t, s \in \mathbb{Z}$ such that $1 = o(g)t + sd$.

Then we have that

$$g = g^{o(g)t+sd} = g^{o(g)t} g^{sd} = (g^s)^d.$$

□

In order to address our problem and study p^k-th powers in A_n, we will distinguish 3 different cases: $p = 2$, $p = 3$ and $p > 3$.

Before starting, we would like to give an elementary definiton.

Definition 1.0.1. *Let σ be a permutation of a symmetric group S_n, $n \geq 1$. The support of σ is defined as*

$$supp(\sigma) = \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}.$$

The following results will be a essential tool in this chapter. They will allow us to join, under certain assumptions, multiple powers into a single one.

Lemma 1.0.1. *Let m be a positive integer and $n \geq 5$. Take $\sigma_1, ..., \sigma_k$ permutations in A_n such that $\sigma_i = \lambda_i^m$ for some $\lambda_i \in A_n$. If $supp(\sigma_i) \cap supp(\sigma_j) = \emptyset$ for every $i \neq j$, then there exists $\lambda \in A_n$, such that $\sigma_1 ... \sigma_k = \lambda^m$ and*

$$supp(\lambda) = \bigcup_{i=1}^{k} supp(\sigma_i).$$

Proof. For each $i \in \{1, ..., k\}$, we have that there exists $\lambda_i \in A_n$ such that $\sigma_i = \lambda_i^m$.

We can assume, without loss of generality that $supp(\lambda_i) = supp(\sigma_i)$, and so, the supports of λ_i and λ_j are disjoint for every $i \neq j$ and we have that λ_i commutes with λ_j for every $i \neq j$.

Then, we have that

$$\prod_{i=1}^{k} \sigma_i = \prod_{i=1}^{k} (\lambda_i)^m = (\prod_{i=1}^{k} \lambda_i)^m.$$

It is enough to take $\lambda = \prod_{i=1}^{k} \lambda_i$.

Let us notice that $supp(\lambda) = \bigcup_{i=1}^{k} supp(\sigma_i)$.

□

The last result can be generalized to the next one.

Theorem 1.0.2. *Let $\sigma_1, ..., \sigma_t$ permutations in A_n such that $\sigma_i = \lambda_{i1}^d ... \lambda_{iN}^d$ for some $N, d \geq 1$. If σ_i and σ_j are disjoint when $i \neq j$ and $supp(\sigma_i) = \cup_{j=1}^N supp(\lambda_{ij})$, then there exist permutations $\lambda_1, ..., \lambda_N$ such that*

$$\sigma_1 ... \sigma_t = \lambda_1^d ... \lambda_N^d.$$

Proof.

It suffices to take $\lambda_1 = \lambda_{11} ... \lambda_{t1}$,..., $\lambda_N = \lambda_{1N} ... \lambda_{tN}$ and take into account that λ_{ij} commutes with λ_{hl} if $i \neq h$. Then, we can use Lemma 1.0.1 to get the result.

Notice that again $\cup_{i=1}^N supp(\lambda_i) = \cup_{j=1}^t supp(\sigma_j)$. □

In what follows, n will be an integer greater than or equal to 5 and k will be an integer greater than or equal to 1.

The aim of this chapter will be to prove that every element in an alternating group A_n can be written as a product of two p^k-th powers in A_n, with p a prime number.

1.1. The case $p = 2$

We will start with the case of $p = 2$. We will consider first those permutations of A_n that can be written as products of cycles of odd length.

Lemma 1.1.1. *Let σ be a permutation that can be written as a product of disjoint cycles of odd length. Then there exists λ in A_n such that $\sigma = \lambda^{2^k}$.*

Proof.

Suppose that $\sigma = (a_1, ..., a_k)$ is a cycle of length odd, $k \geq 3$.

Since $gcd(2, o(\sigma)) = 1$, we can apply Lemma 1.0.1 to get that $\sigma = (\sigma^s)^{2^k}$ for some $s \geq 1$. Clearly, $supp(\sigma) = supp(\sigma^s)$. □

Lemma 1.1.2. *Let σ be a permutation in A_n that can be written as a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{2^k} \eta^{2^k}$.*

Proof. Suppose initially that $\sigma = (a_1, ..., a_{2i})(a_{2i+1}, ..., a_{2r})$ is a permutation in A_n that is a product of two cycles of even length. It is enough to rewrite σ as $\sigma = \xi_1 \eta_1$, where $\xi_1 = (a_1, a_2, ..., a_{2i+1})$ and $\eta_1 = (a_{2i}, a_{2i+1}, ..., a_{2r})$.

By Lemma 1.1.1 there exist elements ξ and η in A_n such that $\xi_1 = \xi^{2^k}$, $\eta_1 = \eta^{2^k}$. So

$$\sigma = \xi^{2^k} \eta^{2^k}.$$

Notice that we can always assume that $supp(\xi), supp(\eta) \subset supp(\sigma)$.

Lemma 1.1.2 is now a direct consequence of Lemma 1.1.1. □

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 1.1.1 and σ_2 satisfies the assumptions of Lemma 1.1.2, a direct application of Theorem 1.0.2 give us the next result.

Theorem 1.1.1. *Every element in an alternating group A_n can be written as a product of two 2^k-th powers in A_n.*

1.2. The case $p \geq 5$

In this section we will address the case $p \geq 5$. We will start considering cycles of odd length in an alternating group A_n.

Lemma 1.2.1. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length, then there exist λ and μ in A_n such that $\sigma = \lambda^{p^k}\mu^{p^k}$.*

Proof. Let's consider first the case in which σ is a single cycle. Suppose that $\sigma = (a_1, ..., a_r)$, with $r \geq 3$ odd. We will distinguish two different cases:

- If p is not a divisor of $o(\sigma)$, the result follows from Lemma 1.1.1, since $\sigma = (\sigma^s)^{p^k}$ for some integer s.
- If p is a divisor of $o(\sigma)$, then we can rewrite σ as

  $$\sigma = (a_1, a_2, a_3)(a_3, a_4, ..., a_r)$$

  as a product of a 3-cycle and a $(r-2)$-cycle.

  But p does not divide neither to 3 nor to $(r-2)$. So, using the previous case, there exist α and β elements in A_n such that

  $$(a_1, a_2, a_3) = \alpha^{p^k} \quad \text{and} \quad (a_3, ..., a_r) = \beta^{p^k}.$$

  So

  $$\sigma = (a_1, a_2, a_3)(a_3, a_4, ..., a_r) = \alpha^{p^k}\beta^{p^k}.$$

Notice that $supp(\alpha), supp(\beta) \subset supp(\sigma)$

Theorem 1.0.2 immediately extends the previous result to permutations that are product of disjoint cycles of odd length.

□

We just solve the case in which a permutation σ in A_n is a product of cycles of odd length. Now, let's consider products of disjoint cycles of even length.

Lemma 1.2.2. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then σ can be written as a product of two p^k-th powers in $A_{supp(\sigma)}$.*

Proof.

To start, consider $\sigma = \sigma_1\sigma_2$ a permutation in A_n, where $\sigma_1 = (a_1, ..., a_{2i})$ and $\sigma_2 = (a_{2i+1}, ..., a_{2r})$. We will consider two different cases:

- If p is not a divisor of $o(\sigma)$, by Lemma 1.0.1, we have that $\sigma = (\sigma^s)^{p^k}$ for some $s \geq 1$.
- If p is a divisor of $o(\sigma)$, let's distinguish two different cases:

  1. If p divides both $o(\sigma_1)$ and $o(\sigma_2)$, then we can rewrite σ as follows:

     $$\sigma = (a_1, a_2)(a_{2i+1}, a_{2i+2})(a_2, ..., a_{2i})(a_{2i+2}, ..., a_{2r}).$$

     Denoting $(a_1, a_2)(a_{2i+1}, a_{2i+2}) = \lambda_1$ and $(a_2, ..., a_{2i})(a_{2i+2}, ..., a_{2r}) = \lambda_2$, it is clear that $\lambda_1 = \lambda_1^{p^k}$ because of $o(\lambda_1) = 2$.
     On the other hand, we have that p is neither a divisor of $o(\sigma_1) - 1$ nor of $o(\sigma_2) - 1$. So, by Lema 1.0.1, we have that λ_2 is a p^k-th power in A_n.
     That is, there exist permutations λ and μ in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$. So

     $$\sigma = \lambda^{p^k}\mu^{p^k}.$$

  2. Suppose that p is a divisor of $o(\sigma_2)$ and not of $o(\sigma_1)$ (the case $p \mid o(\sigma_1)$ and $p \nmid o(\sigma_2)$ is similar). We can rewrite σ as

     $$\sigma = \sigma_1(a_{2i+1}, a_{2i+2})(a_{2i+2}, ..., a_{2r}).$$

     Denoting $\lambda_1 = \sigma_1(a_{2i+1}, a_{2i+2})$ and $\lambda_2 = (a_{2i+2}, ..., a_{2r})$, we have that p is not a divisor of $o(\lambda_1)$ and that p is not a divisor of $o(\lambda_2) = o(\sigma_2) - 1$.
     So, applying Lemma 1.0.1 to λ_1 and to λ_2 we have that there exist λ and μ permutations in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$.
     So, we have that

     $$\sigma = (\lambda)^{p^k}(\mu)^{p^k}.$$

□

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 1.2.1 and σ_2 satisfies the assumptions of Lemma 1.2.2, a direct application of Theorem 1.0.2 gives an analogue of Theorem 1.1.1 in the case $p \geq 5$.

Theorem 1.2.1. *Let p be a prime number greater than 3. Every element in an alternating group A_n can be written as a product of two p^k-th powers in A_n.*

1.3. The case $p = 3$

We will prove that for every natural number $k \geq 1$, every element in A_n, can be written as a product of two 3^k-th powers.

Let's start with the study of cycles of odd length.

Lemma 1.3.1. *Every cycle σ in A_n with odd length $s \geq 3$ can be written as a product of two 3^k-th powers in A_n*

Proof. Take $\sigma = (a_1, ..., a_s)$, with $s \geq 3$ odd. We distinguish three different cases:

1. If 3 does not divide to $o(\sigma)$ we can apply Lemma 1.0.1 to get that $\sigma = (\sigma^t)^{3^k}$ for some $t \geq 1$.

2. If $3 \mid o(\sigma) = s$ and $s \geq 9$, we can rewrite σ as a product of two cycles

   $$\sigma := (a_1, ..., a_5)(a_5, ..., a_s),$$

   one of length 5 and the other one of length $s - 4$. Clearly 3 does not divide $s - 4$.

   Denoting $\lambda_1 = (a_1, ..., a_5)$ and $\lambda_2 = (a_5, ..., a_s)$, we have that $\lambda_1 = (\lambda_1^r)^{3^k}$ and $\lambda_2 = (\lambda_2^t)^{3^k}$ for some $r, t \geq 1$.

   So,

   $$\sigma = (\lambda_1^r)^{3^k}(\lambda_2^t)^{3^k}.$$

   Notice that $\lambda_1, \lambda_2 \in A_{supp(\sigma)}$.

3. Suppose $s = 3$. Assume $\sigma = (a_1, a_2, a_3)$ and take the permutation $x := (a_1, a_5, a_3, a_4, a_2)$ and $y := (a_1, a_3, a_5, a_2, a_4)$ in A_n (Remember that $n \geq 5$). Then we have that $\sigma = yx$, and, by the first case, there exist λ_1 and λ_2 in A_n such that $x = \lambda_1^{3^k}$ and $y = \lambda_2^{3^k}$, that is

   $$\sigma = \lambda_2^{3^k}\lambda_1^{3^k}.$$

□

Remark: If σ is a 3-cycle, $A_{supp(\sigma)} \simeq A_3 \leq A_4$, it is impossible to write σ as a product of two 3^k-th powers neither in A_3 nor A_4.

Indeed, A_3 is an abelian group of order 3 and $A_4^3 = V$, where V is the 4-Klein group that consists of the identity and all products of two disjoint transpositions.

We will need, at least, 5 symbols to write a 3-cycle as a product of two 3^k-powers, for every $k \geq 1$. That's why we have to be careful when using Lemma 1.0.1, in case that a 3-cycle is involved in a permutation σ.

The problem does not appear if only cycles of odd length greater than or equal to 5 appear as we show in the next result.

Corollary 1.3.2. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length greater than* 3*. Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Now, we are going to study what happen when we work with 3-cycles. First of all, we will study the case in which we only have 3-cycles, but more than one.

Lemma 1.3.3. *Let σ be a permutation in A_n that is a product of r disjoint 3-cycles, $r \geq 2$. Then there exist λ and μ in $A_{supp(\sigma)}$ such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Proof. Suppose $\sigma = \sigma_1 ... \sigma_r$, such that σ_i is a 3-cycle for every $i \in \{1, ..., r\}$, $r \geq 2$ and σ_i, σ_j disjoint if $i \neq j$.

- If $r = 2$, suppose that

  $$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6).$$

  Then σ can be rewritten as

  $$\sigma = \xi_1 \xi_2,$$

  where $\xi_1 = (a_1, a_2)(a_4, a_5)$ and $\xi_2 = (a_2, a_3)(a_5, a_6)$.

  Since $o(\xi_1) = 2 = o(\xi_2)$ it follows from Lemma 1.0.1 that

  $$\sigma = (\xi_1^{s_1})^{3^k}(\xi_2^{s_2})^{3^k}.$$

  Notice that $\xi_1, \xi_2 \in A_{supp(\sigma)}$.

- For r even, the result follows immediately from Theorem 1.0.2 and the case $r = 2$.

- If $r = 3$,

  $$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)(a_7, a_8, a_9).$$

Now, we can rewrite $\sigma = \lambda_1\lambda_2$, with $\lambda_1 = (a_1, a_6, a_9, a_5, a_8, a_2, a_3)$ and $\lambda_2 = (a_1, a_8, a_6, a_4, a_9, a_7, a_5)$.

Since $o(\lambda_1) = 7 = o(\lambda_2)$, by Lemma 1.0.1 $\lambda_1 = (\lambda_1^{l_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{l_2})^{3^k}$. So

$$\sigma = (\lambda_1^{l_1})^{3^k}(\lambda_2^{l_2})^{3^k}.$$

Notice that $\lambda_1, \lambda_2 \in A_{supp(\sigma)}$.

- If r is odd, $r \geq 5$, then we can consider the product of the first three 3-cycles and the rest of the 3-cycles in pairs.

  Now the result for σ follows immediately from Theorem 1.0.2 and the previous cases.

□

Once we have solved the last result, we can study the case in which σ is a product of disjoint cycles of odd length.

Lemma 1.3.4. *Let σ be a permutation that is a product of disjoint cycles of odd length.Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Proof. If at least two 3-cycles appear, it follows from Theorem 1.0.2 and Lemmas 1.3.1 and 1.3.3. So let us assume that only one 3-cycle appears, in the expression of σ as product of cycles of odd length.

Let's write $\sigma = \sigma_1\alpha_1...\alpha_r$, with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_i a cycle of odd length greater than 3 for every $i \in \{1, ..., r\}$.

We can apply Lemma 1.3.1 and Theorem 1.0.2 to $\alpha_2...\alpha_r$ to get that there exist β, γ in A_n such that $supp(\beta, \gamma) \subset \cup_{i=2}^{r} supp(\alpha_i)$ such that

$$\alpha_2...\alpha_r = \beta^{3^k}\gamma^{3^k}.$$

Consider now $\sigma_1\alpha_1 = (a_1, a_2, a_3)(a_4, a_5, ..., a_s)$, with $s \geq 8$ even. We distinguish two cases:

- If 3 does not divide to $s - 4$, we can rewrite $\sigma_1\alpha_1$ as follows:

  $$\sigma_1\alpha_1 = (a_1, a_2)(a_4, a_5)(a_2, a_3)(a_5, ..., a_s).$$

  If we denote $\lambda_1 = (a_1, a_2)(a_4, a_5)$ and $\lambda_2 = (a_2, a_3)(a_5, ..., a_s)$, we have that 3 does not divide neither to $o(\lambda_1) = 2$ nor to $o(\lambda_2) = s - 4$.

  By Lemma 1.0.1, $\lambda_1 = (\lambda_1^{m_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{m_2})^{3^k}$, for some $m_1, m_2 \geq 1$.

  So, we have that

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

- If 3 is a divisor of $s-4$, we can rewrite $\sigma_1\alpha_1$ as follows:

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2,$$

  where $\lambda_1 = (a_1, a_2, a_3, a_4, a_5)$ and $\lambda_2 = (a_3, a_5, a_6, ..., a_s)$. Then 3 does not divide neither to $o(\lambda_1) = 5$ nor to $o(\lambda_2) = (s-3)$.

  Again by Lemma 1.0.1 we get that $\lambda_1 = (\lambda_1^{n_1})^{3^k}$ and that $\lambda_2 = (\lambda_2^{n_2})^{3^k}$, for some $n_1, n_2 \geq 1$.

  Consequently

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

  Theorem 1.0.2 finishes the proof of this Lemma.

□

To give an analogue of 1.2.1 for $p = 3$, we still need to study products of cycles of even length.

Lemma 1.3.5. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof. The proof follows the same lines of the proof of Lemma 1.2.2. □

If σ is a permutation in A_n, we can write it as

$$\sigma = \sigma_1...\sigma_r\gamma_1...\gamma_s(\alpha_1\alpha_2)...(\alpha_{2l-1}\alpha_{2l}),$$

where each σ_i is a 3-cycle, $i \in \{1, ..., 2r\}$, γ_j is a cycle of odd length greater or equal than 5, $j \in \{1, ..., s\}$, and α_k is a cycle of even length for every k, $k \in \{1, ..., 2l\}$.

In the case $s = 0$, $r = 1$ and $l \geq 1$ we will find a problem. Notice that in this case σ_1 is a product of two 3^k-powers, but we need to involve two symbols that do not appear in $supp(\sigma_1)$, so Theorem 1.0.2 can not be directly applied. The next results solve this problem.

Lemma 1.3.6. *Let σ be a permutation in A_n that is a product of a single 3-cycle and two disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof.

Suppose that σ can be written as follows:

$$\sigma = \sigma_1(\alpha_1\alpha_2),$$

with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_1, α_2 are cycles of even length, $\alpha_1 = (b_1, ..., b_{2i})$, $\alpha_2 = (b_{2i+1}, ..., b_{2t})$.

We distinguish four different cases:

- If 3 divides to both $o(\alpha_1)$ and $o(\alpha_2)$, or equivalently $3 \mid i$ and $3 \mid t$, we rewrite σ as $\sigma = \lambda_1\lambda_2$, where $\lambda_1 = (a_1, a_2)(b_1, b_2)(b_{2i+1}, ..., b_{2t-1})$ and $\lambda_2 = (a_2, a_3)(b_{2t-1}, b_{2t})(b_2, ..., b_{2i})$.

  But 3 does not divide neither to $o(\lambda_1) = 2(2(t-i)-1)$ nor to $o(\lambda_2) = 2(2i-1)$. So Lemma 1.0.1 gives the result, since $\lambda_1 = (\lambda_1^p)^{3^k}$ and $\lambda_2 = (\lambda_2^q)^{3^k}$, for some $p, q \in \mathbb{Z}$.

- If 3 divides to $o(\alpha_1)$ but does not divide to $o(\alpha_2)$, that is $3 \mid i$, but $3 \nmid t$, we rewrite σ as follows:

  $$\sigma = \lambda_1\lambda_2,$$

  where $\lambda_1 = (a_1, a_2, a_3, b_1)(b_{2i+1}, ..., b_{2t})$ and $\lambda_2 = (a_3, b_1, b_2, ..., b_{2i})$.

  Now, 3 does not divide to $(2i+1) = o(\lambda_2)$, so we can apply Lemma 1.0.1.

  Similarly, 3 does not divide to $4(t-i) = o(\lambda_1)$. we can use again Lemma 1.0.1.

  So,

  $$\sigma = (\lambda_1^v)^{3^k}(\lambda_2^u)^{3^k},$$

  for some integers u, v.

- If 3 divides to $o(\alpha_2)$ but 3 does not divide to $o(\alpha_1)$, the proof is similar.

- If 3 does not divide neither to $o(\alpha_2)$ nor to $o(\alpha_1)$, we rewrite σ as follows

  $$\sigma = (a_1, a_2, a_3, b_1, b_2)(a_3, b_2, ..., b_{2i})(b_{2i+1}, ..., b_{2t}).$$

  Denote $\lambda_1 = (a_1, a_2, a_3, b_1, b_2)$ and $\lambda_2 = (a_3, b_2, ..., b_{2i})(b_{2i+1}, ..., b_{2t})$.

  Since 3 does not divide to $o(\lambda_1) = 5$ and 3 does not divide to $o(\lambda_2) = mcm(2i, 2t-2i)$, the result follows immediately from Lemma 1.0.1.

  This finishes the proof of Lemma 1.3.6.

□

At this point we are in a position to give the main result of this section.

Theorem 1.3.1. *Every element in an alternating group A_n can be written as a product of two 3^k-th powers in A_n.*

We can join all we have done to give a corollary in order to finish the chapter.

Corollary 1.3.7. *Let p be a prime number. Every element in an alternating group A_n can be written as a product of two p^k-th powers in A_n.*

Capítulo 2

Producto de dos palabras de Engel

En 1951 O. Ore ([23]) probó que todo elemento de un grupo Alternado A_n, con $n \geq 5$, es un conmutador en A_n. Notemos que lo que este resultado nos dice es que si tomamos la palabra $\tau := x_1^{-1}x_2^{-1}x_1x_2$ en el grupo libre de rango 2, $\mathcal{F}_2$, entonces $\tau(A_n) = A_n$, para todo $n \geq 5$.

Además, Ore conjeturó que este mismo resultado era también cierto para todo grupo simple G, problema que es conocido como Conjetura de Ore.

En 2010, M. W. Liebeck, E. A. O'Brien, A. Shalev y P. H. Tiep [16] terminaron la demostración de la Conjetura de Ore. Probaron que para todo grupo simple finito G, se tiene que $G = \tau(G)$.

La pregunta que surge ahora es: ¿Qué ocurre sin el lugar de τ escogemos otro elemento del grupo libre $\mathcal{F}_2$?

Comencemos definiendo el subgrupo verbal de un grupo G respecto a una palabra ω. Sea r un número natural, $\mathcal{F}_r$ el grupo libre asociado de rango r y ω una palabra reducida de $\mathcal{F}_r$.

Podemos definir la aplicación asociada a la palabra como

$$\begin{aligned}\tilde{\omega} : \overbrace{G \times \cdots \times G}^{r} &\longrightarrow G \\ (g_1, ..., g_r) &\mapsto \tilde{\omega}(g_1, ..., g_r).\end{aligned}$$

Definición 2.0.1. *Dada una palabra reducida ω en el grupo libre de rango r, $\mathcal{F}_r$, G un grupo y $\tilde{\omega} : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$, el subgrupo verbal de G asociado a ω se define como el grupo generado por el conjunto $\omega(G) = Im\tilde{\omega} = \{\tilde{\omega}(g_1, ..., g_r) \mid g_1, ..., g_r \in G\}$.*

Definición 2.0.2. *Sea m un entero positivo. La palabra de Engel de longitud*

m se define como el elemento del grupo libre $\mathcal{F}_2$

$$E_m = [...[x, \overbrace{y], y}^{m}], ..., y].$$

Es claro que el subgrupo verbal de G asociado a E_m es un subgrupo normal de G al que denominaremos subgrupo de Engel de longitud m.

Nuestro objetivo en este capítulo es proporcionar una primera respuesta para grupos Alternados simples. Probaremos que todo elemento en A_n, con $n \geq 5$, es un producto de, a lo sumo, dos palabras de Engel de longitud arbitraria, esto es

$$A_n = E_m(A_n)E_m(A_n),$$

para todo par de números naturales $m \geq 2$ y $n \geq 5$.

2.1. El caso $n = 2$

Dado que el subgrupo verbal asociado a E_m es un subgrupo normal en A_n y A_n es un grupo simple no abeliano si $n \geq 5$, es claro que dicho subgrupo coincide con A_n. Para probarlo, basta notar que $E_m(x, y)$ no es una identidad de A_n para ningún m.

Por tanto, cada elemento de A_n es un producto de un número finito de elementos, cada uno de ellos en $Im(\tilde{\omega})$, con $\tilde{\omega} = E_m(x, y)$.

El objetivo de esta sección será probar que todo elemento del grupo alternado A_n, con $n \geq 5$, se puede expresar como producto de dos palabras de Engel de longitud 2 en A_n.

Observemos el comportamiento de los grupos alternados A_n con $n < 5$.

Si $n \in \{1, 2, 3\}$, el grupo A_n es abeliano y por lo tanto cualquier conmutador de dos elementos de A_n será la identidad. Por lo que, $E_2(x, y) = e$ para todos $x, y \in A_n$.

Si $n = 4$, sabemos que el subgrupo derivado de A_4 es el $4-$grupo de Klein, dado por

$$V = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

Así, tendremos que $E_2(A_4) \subset [V, A_4] = V$.

Luego los únicos elementos de A_4 que pueden escribirse como producto de dos palabras de Engel de longitud dos (y que de hecho, se pueden expresar sólo con una palabra) son los elementos del $4-$grupo de Klein, es decir, $E_2(A_4) = V$.

En primer lugar daremos algunos resultados preliminares que serán una herramienta importante en este trabajo, ya que, bajo ciertas condiciones, nos

permitirán unir dos palabras de Engel de longitud 2 en una única palabra de la misma longitud.

En lo que sigue y salvo que se especifique lo contrario, el grado n del grupo simétrico será un entero mayor o igual que 5 y la longitud m de la palabra de Engel $E_m(x, y)$ será un entero mayor o igual que 2.

Lema 2.1.1. *Sean $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in S_n$ tales que σ_1, σ_2 conmutan con σ_3, σ_4. Entonces, $E_2(\sigma_1\sigma_3, \sigma_2\sigma_4) = E_2(\sigma_1, \sigma_2)E_2(\sigma_3, \sigma_4)$.*

Demostración. Puesto que σ_1, σ_2 conmutan con σ_3, σ_4, se tiene que todo elemento de $\langle\sigma_1, \sigma_2\rangle$ conmuta con todo elemento de $\langle\sigma_3, \sigma_4\rangle$. En particular, se tiene que $[\sigma_1, \sigma_2]$ conmuta con $[\sigma_3, \sigma_4]$ y que $E_2(\sigma_1, \sigma_2)$ conmuta con $E_2(\sigma_3, \sigma_4)$.

Por otro lado,

$$\begin{aligned}[\sigma_1\sigma_3, \sigma_2\sigma_4] &= \sigma_3^{-1}\sigma_1^{-1}\sigma_4^{-1}\sigma_2^{-1}\sigma_1\sigma_3\sigma_2\sigma_4 = \sigma_3^{-1}\sigma_4^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2\sigma_3\sigma_4 = \\ &= \sigma_3^{-1}\sigma_4^{-1}[\sigma_1, \sigma_2]\sigma_3\sigma_4 = \sigma_3^{-1}\sigma_4^{-1}\sigma_3\sigma_4\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 = \\ &= [\sigma_3, \sigma_4][\sigma_1, \sigma_2] = [\sigma_1, \sigma_2][\sigma_3, \sigma_4].\end{aligned}$$

Por tanto,

$$E_2(\sigma_1\sigma_3, \sigma_2\sigma_4) = [[\sigma_1\sigma_3, \sigma_2\sigma_4], \sigma_2\sigma_4] = [[\sigma_1, \sigma_2][\sigma_3, \sigma_4], \sigma_2\sigma_4],$$

y, $[\sigma_1, \sigma_2]$ y σ_2 conmutan con $[\sigma_3, \sigma_4]$ y σ_4. Aplicando el argumento anterior, tendremos que:

$$E_2(\sigma_1\sigma_3, \sigma_2\sigma_4) = [[\sigma_1, \sigma_2], \sigma_2][[\sigma_3, \sigma_4], \sigma_4] = E_2(\sigma_1, \sigma_2)E_2(\sigma_3, \sigma_4).$$

□

Corolario 2.1.2. *Sean $\sigma_1, ..., \sigma_{2r} \in S_n$ tales que para todo $i \neq j \in \{1, ..., r\}$, los soportes de $\sigma_{2i-1}, \sigma_{2i}$ son disjuntos con los soportes de $\sigma_{2j-1}, \sigma_{2j}$. Entonces se tiene que*

$$E_2(\sigma_1, \sigma_3, ..., \sigma_{2r-1}, \sigma_2\sigma_4, ..., \sigma_{2r}) = E_2(\sigma_1, \sigma_2)E_2(\sigma_3, \sigma_4)...E_2(\sigma_{2r-1}, \sigma_{2r}).$$

Demostración. Basta notar que permutaciones con soportes disjuntos conmutan y usar el lema 2.1.1. □

Dada una permutación τ en el grupo simétrico S_n, denotemos al soporte de τ como

$$sop(\tau) := \{i \in \{1, ..., n\} \mid \tau(i) \neq i\}.$$

Claramente, τ puede ser vista como una permutación en $S_{sop(\tau)}$. Es evidente que si $s \geq n$ se tiene que $A_n \leq A_s$ y por tanto, si σ es una permutación en A_n que puede ser escrita como una palabra de Engel (o como un producto de dos palabras de Engel) en A_n, también será una palabra (o un producto de dos palabras) en A_s.

Nota. Consideraremos permutaciones pares σ cuya descomposición $\sigma = \sigma_1 ... \sigma_t$ como producto de ciclos disjuntos es de uno de los cuatro tipos siguientes:

I Todo σ_i es un ciclo de longitud mayor que 3.

II Hay $r \geq 2$ 3-ciclos: $\sigma_1, ..., \sigma_r$.

III $t = 2s$ y la longitud de σ_i es par para todo $i \in \{1, ..., 2s\}$

IV Hay exactamente un 3-ciclo, σ_i.

Es claro que una permutación par o es de uno de los tipos anteriores o es un producto de permutaciones disjuntas de los tipos (I) y (III).

El siguiente resultado, que puede resultar obvio, será usado con mucha frecuencia durante el desarrollo de los Capítulos 2 y 3.

Lema 2.1.3. *Sea σ una permutación del grupo Alternado A_n. Si σ es un elemento de $E_m(A_n)$, con $m \geq 1$, se tiene que todo elemento de $Cl_{S_n}(\sigma)$ puede ser escrito como una palabra de Engel de longitud m en A_n.*

Demostración. Si σ es una palabra de Engel de longitud 2 en A_n se tiene que existen permutaciones α y β en A_n tales que $\sigma = E_m(\alpha, \beta)$.

Basta observar que para toda permutación θ en el grupo Simétrico S_n se verifica que

$$\sigma^\theta = E_m(\alpha^\theta, \beta^\theta).$$

□

Este lema nos indica que para probar que una permutación σ está en $E_m(A_n)$ basta mostrar que una permutación cualquiera del mismo tipo que σ es un elemento de $E_m(A_n)$.

El primer caso que se tratará será cuando $\sigma \in A_n$ sea un producto de 2-ciclos.

Lema 2.1.4. *Sea $\sigma \in A_4$ una permutación que es un producto de dos trasposiciones disjuntas. Entonces σ es una palabra de Engel de longitud dos en A_4.*

Demostración. Sean $\tau = (a, c, b)$ y $\zeta = (a, d, b)$. Es inmediato comprobar que $(a, d)(b, c) = E_2(\tau, \zeta)$ y que $sop(\sigma) = \{a, b, c, d\} = sop(\tau) \cup sop(\zeta)$.

Basta aplicar el lema 2.1.3 para extender el resultado a todo elemento de $Cl_{A_4}(\sigma)$. □

Los dos resultados que siguen prueban que los ciclos en A_n, $n \geq 5$, son palabras de Engel de longitud 2 ó un producto de dos de ellas.

Lema 2.1.5. *Consideremos p un número impar, con $p \geq 3$, y sea σ un p-ciclo en A_p. Entonces σ es una palabra de Engel de longitud dos en S_p, y por lo tanto, lo será también en A_{p+2}.*

Demostración. Sin pérdida de generalidad podemos suponer que $\sigma := (1, ..., p)$.

Como $\#sop(\sigma) = p$, podemos considerar $\sigma \in A_p$. Teniendo en cuenta que $o(\sigma) = p$ y que $(2, p) = 1$, podemos concluir que σ^2 será también un p-ciclo. De este modo, obtenemos que σ y σ^2 son conjugados en S_p.

Por tanto, existe $\tau \in S_p$ tal que $\sigma^\tau = \sigma^2$, de dónde se obtiene que $[\sigma, \tau] = \sigma$, concluyendo finalmente que $\sigma = E_2(\sigma, \tau)$.

Ahora es suficiente con usar la bien conocida incrustación de S_p en A_{p+2}, esto es:

Si $\tau \in A_p \subset A_n$, tendremos que $\sigma \in E_2(A_p)$.

Si $\tau \in S_p \setminus A_p$, podemos considerar la permutación $\zeta = \tau(p + 1, p + 2) \in A_{p+2}$ y tendremos que $\sigma = E_2(\sigma, \zeta) \in E_2(A_{p+2})$. □

Dado σ un ciclo de longitud impar en A_n, el caso en el que σ deja dos cifras fijas está resuelto, puesto que el lema anterior nos asegura que podremos escribir σ como una única palabra de Engel de longitud 2 en A_n.

En el siguiente resultado estudiaremos qué ocurre cuando σ deja menos de dos cifras fijas.

Lema 2.1.6. *Sea p un número impar, $p \geq 5$. Todo p-ciclo en A_n se puede escribir como producto de dos palabras en Engel de longitud dos en A_p.*

Demostración. Podemos suponer, sin pérdida de generalidad, que $\sigma = (1, ..., p)$. Entonces tendremos que $\sigma = \sigma_1\sigma_2$, con $\sigma_1 = (1, 2, 3)$ y $\sigma_2 = (3, 4, ..., n)$. Notemos que σ_1 y σ_2 son ciclos de longitud mayor o igual que 3 en A_p.

Por el lema 2.1.5, podemos asegurar que existen $\tau_1, \tau_2 \in S_n$, con $sop(\tau_1) \subset sop(\sigma_1)$ y $sop(\tau_2) \subset sop(\sigma_2)$, verificando que $\sigma_1 = E_2(\sigma_1, \tau_1)$ y $\sigma_2 = E_2(\sigma_2, \tau_2)$.

Si τ_1 es una permutación impar, sustituiremos τ_1 por $\theta_1 = \tau_1(n - 1, n)$. Así, $\sigma_1 = E_2(\sigma_1, \theta_1)$, con $\theta_1 \in A_p$.

De forma análoga, si τ_2 es impar, sustituiremos τ_2 por $\theta_2 = \tau_2(1, 2)$, concluyendo que $\sigma_2 = E_2(\sigma_2, \theta_2)$, con $\theta_2 \in A_p$.

De este modo,

$$\sigma = \sigma_1\sigma_2 = E_2(\sigma_1, \theta_1)E_2(\sigma_2, \theta_2),$$

con $\sigma_1, \sigma_2, \theta_1, \theta_2 \in A_p$.

□

Puesto que hemos probado que todo ciclo σ en A_n cuya longitud m sea mayor o igual que 5 se puede escribir como producto de dos palabras en Engel de longitud 2 en el propio grupo A_m, el lema 2.1.6 resuelve el problema para permutaciones de tipo (I)

Dado que los lemas anteriores excluyen a los 3-ciclos, abordaremos en el siguiente resultado el estudio de los 3-ciclos.

Lema 2.1.7. *Sea σ una permutación en A_n, $n = sop(\sigma)$, que se puede escribir como producto de dos o más 3-ciclos disjuntos. Entonces, σ es un producto de dos palabras de Engel de longitud 2 en A_n.*

Demostración. Sabemos que si $\sigma = (a, b, c) \in A_n$, se tiene que $\sigma = E_2(\sigma, (a, b))$, pues $\sigma^{(a,b)} = \sigma^2$.

Sea $\sigma := \sigma_1...\sigma_r \in A_n$, con $r \geq 2$ y σ_i un $3-$ciclo para todo $i \in \{1, ..., r\}$. Notemos que σ_i y σ_j son disjuntos para todo $i \neq j$.

Si r es par, agrupando los $3-$ciclos por parejas, basta probar el resultado para el caso $r = 2$ y posteriormente aplicar el corolario 2.1.2.

Supongamos entonces que $\sigma = (a, b, c)(d, e, f)$. Como $(a, b, c) = E_2((a, b, c), (a, b))$ y $(d, e, f) = E_2((d, e, f), (d, e))$, tendremos que

$$\begin{aligned} \sigma &= E_2((a, b, c), (a, b))E_2((d, e, f), (d, e)) = \\ &= E_2((a, b, c)(d, e, f), (a, b)(d, e)) \in E_2(A_6). \end{aligned}$$

Si r es impar (y mayor o igual que 3, por hipótesis) podemos agrupar los tres primeros 3-ciclos por un lado, y el resto de 3-ciclos por parejas por otro. De nuevo, teniendo en cuenta el corolario 2.1.2, basta probar que un producto de tres 3-ciclos se puede expresar como producto de dos palabras de Engel de longitud dos en A_9.

Supongamos que $\zeta = (a, b, c)(d, e, f)(g, h, i)$, así, tendremos que

$$\zeta = E_2((a, b, c), (a, b))E_2((d, e, f), (d, e))E_2((g, h, i), (g, h)).$$

Pero aplicando el lema 2.1.1 a las dos primeras palabras de Engel de la expresión anterior, tendremos que

$$\begin{aligned} \zeta &= E_2((a, b, c)(d, e, f), (a, b)(d, e))E_2((g, h, i), (g, h)) = \\ &= E_2((a, b, c)(d, e, f), (a, b)(d, e))E_2((g, h, i), (a, b)(g, h)) \in E_2(A_n)E_2(A_n). \end{aligned}$$

□

Conviene notar que si no exigimos que las permutaciones involucradas en la palabra pertenezcan la grupo alternado, tendremos que

$$\zeta = E_2((a,b,c)(d,e,f)(g,h,i),(a,b)(d,e)(g,h)) \in E_2(S_9)$$

De hecho, se ha probado algo más. Si tenemos una permutación que se puede escribir como producto de un número par de 3-ciclos, cada pareja de 3-ciclos es una palabra de Engel de longitud 2 en el grupo alternado correspondiente isomorfo a A_6, como se ha podido observar en la demostración anterior. Así, gracias de nuevo al corolario 2.1.2, tendremos el siguiente resultado.

Corolario 2.1.8. *Sea σ una permutación en A_n, $n = sop(\sigma)$, que se puede escribir como producto de un número par 3-ciclos disjuntos. Entonces, σ es una palabra de Engel de longitud dos en A_n.*

Si σ es una permutación en A_n, con $n = sop(\sigma)$, que se puede escribir como producto de ciclos disjuntos de longitud impar y el número de 3-ciclos es distinto de uno, tendremos que σ es un producto de dos palabras de Engel de longitud dos en A_n. Esto se sigue de manera inmediata de los lemas 2.1.6 y 2.1.7 y del corolario 2.2.2. De este modo, el estudio de permutaciones de tipo (II) queda resuelto.

Queda considerar el caso en el que la expresión de σ involucra exactamente un 3-ciclo (tipo (IV)) o sólo pares de elementos de longitud par (tipo (III)). El siguiente resultado nos resuelve la cuestión para permutaciones del tipo (III).

Lema 2.1.9. *Sea σ una permutación en A_n, con $n = sop(\sigma)$, que se puede escribir como producto de dos ciclos disjuntos de longitud par, entonces σ es producto de dos palabras de Engel de longitud dos en A_n.*

Demostración. El lema 2.1.4 nos resuelve el caso en el que σ es producto de dos trasposiciones. Sea entonces $\sigma = \sigma_1\sigma_2$, con σ_1, σ_2 ciclos de longitud par. Supongamos que $\sigma_1 = (a_1, ..., a_r)$ y $\sigma_2 = (b_1, ..., b_t)$, con r, t pares.

Si $r, t \geq 4$, podemos reescribir σ_1 y σ_2 de la siguiente manera:

$$\begin{aligned} \sigma_1 &= (a_1, ..., a_r) = (a_1, ..., a_{r-1})(a_{r-1}, a_r) := \zeta_1(a_{r-1}, a_r); \\ \sigma_2 &= (b_1, ..., b_t) = (b_1, ..., b_{t-1})(b_{t-1}, b_t) := \zeta_2(b_{t-1}, b_t). \end{aligned}$$

Aplicando el lema 2.1.5 tendremos que existen $\lambda_1 \in S_{p-1}$ y $\lambda_2 \in S_{t-1}$, tales que $E_2(\zeta_i, \lambda_i) = \zeta_i$, con $i \in \{1, 2\}$

Si λ_1, λ_2 son pares (ó respectivamente λ_1, λ_2 son impares), basta tener en cuenta que los soportes de σ_1 y σ_2 son disjuntos y aplicar el corolario 2.1.2, para obtener que

$$\zeta_1\zeta_2 = E_2(\zeta_1\zeta_2, \lambda_1\lambda_2) \in E_2(A_n).$$

Si λ_1 es par y λ_2 es impar (o respectivamente λ_1 is impar y λ_2 es par), basta ver que $\zeta_2 = E_2(\zeta_2, \lambda_2(a_r, b_t)) \in E_2(A_n)$. Como ζ_1, λ_1 conmutan con $\zeta_2, \lambda_2(a_r, b_t)$, pues tienen soportes disjuntos, basta aplicar el lema 2.1.1 para obtener que

$$\zeta_1\zeta_2 = E_2(\zeta_1\zeta_2, \lambda_1\lambda_2(a_r, b_t)) \in E_2(A_n).$$

Aplicando el lema 2.1.4 a $(a_{r-1}, a_r)(b_{t-1}, b_t)$, se tiene que existen $\tau, \theta \in A_n$ tales que

$$(a_{r-1}, a_r)(b_{t-1}, b_t) = E_2(\tau, \theta) \in E_2(A_n).$$

Como $\sigma = \sigma_1\sigma_2 = \zeta_1\zeta_2(a_{r-1}, a_r)(b_{t-1}, b_t)$, aplicando lo anterior a $\zeta_1\zeta_2$ por un lado, y a $(a_{r-1}, a_r)(b_{t-1}, b_t)$ por otro, tendremos que $\sigma \in E_2(A_n)E_2(A_n)$.

Falta considerar el caso en el que la longitud de uno de los ciclos sea 2. Sin pérdida de generalidad, supongamos que $t = 2$. Así, tendremos que $\sigma = \sigma_1(b_1, b_2) = \zeta_1(a_{r-1}, a_r)(b_1, b_2)$. Como $\zeta_1 = E_2(\zeta_1, \lambda_1)$, tendremos dos casos.

- Si $\lambda_1 \in A_n$, entonces $\xi_1 = E_2(\zeta_1, \lambda_1) \in E_2(A_n)$, y por tanto $\sigma \in E_2(A_n)$, pues $(a_{r-1}, a_r)(b_1, b_2) \in E_2(A_n)$ por el lema 2.1.4.

- Si $\lambda_1 \in S_n \setminus A_n$, entonces sustituimos λ_1 por $\beta_1 = \lambda_1(b_1, b_2) \in A_n$. Así, tendremos que $\zeta_1 = E_2(\zeta_1, \beta_1) \in E_2(A_n)$ y de nuevo, $\sigma \in E_2(A_n)E_2(A_n)$.

□

El lema 2.1.9 resuelve el caso de permutaciones de tipo (III). Notemos que en la construcción de las palabras de Engel de longitud dos del caso anterior, los soportes de las permutaciones que forman la palabra siempre están contenidos en el soporte de la permutación inicial.

Sólo queda considerar el caso en que σ involucre un único 3-ciclo. El siguiente resultado resuelve esta cuestión.

Lema 2.1.10. *Sea σ una permutación en A_n de tipo (III), con $n = sop(\sigma)$. Entonces σ es un producto de dos palabras de Engel de longitud 2 en A_n.*

Demostración. Sea σ una permutación en A_n que puede ser expresada como

$$\sigma = \sigma_1\tilde{\sigma_2}\tilde{\sigma_3},$$

siendo σ_1 un 3-ciclo, $\tilde{\sigma_2}$ un producto de ciclos de longitud impar y mayor que 3 y $\tilde{\sigma_3}$ un producto de un número par de ciclos de longitud par. Estudiaremos dos casos distintos:

1. Si $\tilde{\sigma_3} = 1$, consideraremos $\sigma = (a,b,c)\tilde{\sigma_2}$. Todo ciclo τ de $\tilde{\sigma_2}$ tiene longitud impar mayor que 3, por lo tanto $\tilde{\sigma_2} = E_2(\tilde{\sigma_2}, \theta)$ es una palabra de Engel de longitud dos en S_m, con $m = \sharp sop(\sigma)$.

   Por otro lado, $\sigma = (a,b,c)\tilde{\sigma_2}$ y $(a,b,c) = E_2((a,b,c),(a,b))$.

   Si $\theta \in S_n \setminus A_n$, $\sigma = E_2(\sigma, \theta(a,b)) \in E_2(A_n)$.

   Si $\theta \in A_n$, entonces basta tomar dos cifras cualesquiera j y k en el $sop(\tilde{\sigma_2})$ para obtener que $\sigma = (a,b,c)\tilde{\sigma_2} = E_2((a,b,c),(a,b)(j,k))E_2(\tilde{\sigma_2}, \theta) \in E_2(A_n)E_2(A_n)$.

2. Si $\tilde{\sigma_3} \neq 1$, sabemos que $(a,b,c)\tilde{\sigma_2} \in E_2(A_n)E_2(A_n)$. Entonces $(a,b,c)\tilde{\sigma_2} = E_2(\theta_1,\eta_1)E_2(\theta_2,\eta_2)$ y $\tilde{\sigma_3} = E_2(\theta_3,\eta_3)E_2(\theta_4,\eta_4)$ gracias al lema 2.1.9, donde $\{\theta_1,\theta_2,\eta_1,\eta_2\}$ son disjuntos con $\{\theta_3,\theta_4,\eta_3,\eta_4\}$.

   De este modo $\sigma = (a,b,c)\tilde{\sigma_2}\tilde{\sigma_3}$ puede ser escrita como

   $$\sigma = E_2(\theta_1,\eta_1)E_2(\theta_2,\eta_2)E_2(\theta_3,\eta_3)E_2(\theta_4,\eta_4),$$

   y aplicando el lema 2.1.1 obtendremos que

   $$\sigma = E_2(\theta_1\theta_3, \eta_1\eta_3)E_2(\theta_2\theta_4, \eta_2\eta_4) \in E_2(A_n)E_2(A_n).$$

□

Este último resultado prueba que las permutaciones de tipo (III) son producto de dos palabras de Engel de longitud 2 en A_n. El resultado para las permutaciones de tipo (I), (II), (III) y (IV) asegura el resultado buscado y que era el objetivo de esta sección.

Teorema 2.1.11. *Toda permutación en A_n se puede escribir como un producto de dos palabras de Engel de longitud dos en A_n.*

2.2. El caso general

Una vez probado el teorema 2.1.11, cabe preguntarse si es posible demostrar un resultado análogo para palabras de Engel de longitud arbitraria.

Del mismo modo que en la sección anterior, conviene mostrar que ocurre cuando trabajamos con un grupo alternado pequeño A_n con $n < 5$. Fijemos $m \in \mathbb{N}$ mayor que dos.

Así, si $n = 1, 2$ tendremos que $\{e\} = A_1 = A_2$. Si $n = 3$, el grupo A_3 será abeliano, y al igual que en el caso de palabras de Engel de longitud dos, $E_m(x,y) = e$ para todo $x, y \in A_3$.

Si $n = 4$, en la sección anterior vimos que $E_2(A_4) = V$. Probaremos que sucede lo mismo para $E_m(A_4)$ en el lema 2.2.3.

Pero antes de enunciar dicho lema, conviene generalizar al caso de palabras de Engel de longitud arbitraria los resultados 2.1.1 y 2.1.2.

Lema 2.2.1. *Consideremos $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in S_n$ tales que σ_1, σ_2 conmutan con σ_3, σ_4. Entonces, para todo $m \in \mathbb{N}$, se tiene*

$$E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) = E_m(\sigma_1, \sigma_2)E_m(\sigma_3, \sigma_4)$$

.

Demostración. Procederemos por inducción sobre m. Los casos $m = 1$ y $m = 2$ están probados en el lema 2.1.1. Supongamos entonces el resultado cierto para $m - 1$, es decir, bajo las hipótesis del enunciado tendremos que

$$E_{m-1}(\sigma_1\sigma_3, \sigma_2\sigma_4) = E_{m-1}(\sigma_1, \sigma_2)E_{n-1}(\sigma_3, \sigma_4).$$

De este modo, tendremos que

$$E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) = [E_{m-1}(\sigma_1\sigma_3, \sigma_2\sigma_4), \sigma_2\sigma_4] = [E_{m-1}(\sigma_1, \sigma_2)E_{m-1}(\sigma_3, \sigma_4), \sigma_2\sigma_4],$$

y como $E_{m-1}(\sigma_1, \sigma_2)$ y σ_2 conmutan con $E_{m-1}(\sigma_3, \sigma_4)$ y σ_4, tendremos que

$$\begin{aligned} E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) &= [E_{m-1}(\sigma_1, \sigma_2)E_{m-1}(\sigma_3, \sigma_4), \sigma_2\sigma_4] = \\ &= [E_{m-1}(\sigma_1, \sigma_2), \sigma_2][E_{m-1}(\sigma_3, \sigma_4), \sigma_4] = \\ &= E_m(\sigma_1, \sigma_2)E_n(\sigma_3, \sigma_4). \end{aligned}$$

□

Corolario 2.2.2. *Sean $\sigma_1, ..., \sigma_{2r}$ permutaciones en S_n tales que σ_{2i-1} conmuta con σ_j para todo $j \neq 2i$ y σ_{2i} conmuta con σ_j para todo $j \neq 2i - 1$. Entonces, para todo $m \in \mathbb{N}$,tendremos que*

$$E_m(\sigma_1\sigma_3...\sigma_{2r-1}, \sigma_2\sigma_4, ..., \sigma_{2r}) = E_m(\sigma_1, \sigma_2)E_m(\sigma_3, \sigma_4)...E_m(\sigma_{2r-1}, \sigma_{2r}).$$

Demostración. Es suficiente con usar el lema 2.2.1. □

Pasemos ahora a enunciar y demostrar un análogo del lema 2.1.4 para el caso de palabras de Engel de longitud arbitraria.

Lema 2.2.3. *Sea $\sigma = (1, 2)(3, 4) \in A_4$. Entonces para todo $m \in \mathbb{N}$, σ es una palabra de Engel de longitud m en A_n.*

Demostración. Basta notar que la sucesión $\{E_m((1,3,4),(1,2,4))\}_{n\geq 2}$ es periódica módulo 3. De hecho, se tiene:

$$\begin{array}{lll} (1,2)(3,4) = E_m((1,3,4),(1,2,4)) & \text{if} & m \equiv 0 \mod(3), \\ (1,2)(3,4) = E_m((1,4,3),(1,2,3)) & \text{if} & m \equiv 1 \mod(3), \\ (1,2)(3,4) = E_m((1,4,2),(1,3,4)) & \text{if} & m \equiv 2 \mod(3). \end{array}$$

□

Pasaremos ahora a tratar el caso de ciclos de longitud impar en A_n, con $n \geq 5$. Para ello, extenderemos el lema 2.1.5 a palabras de Engel de longitud arbitraria.

Lema 2.2.4. *Sea σ un ciclo en A_n de longitud impar r y mayor o igual que 3. Entonces, σ se puede escribir como una única palabra de Engel de longitud arbitraria en A_{r+2}.*

Demostración. Aplicando el lema 2.1.5, sabemos que existe $\tau \in A_{r+2}$ tal que $[\sigma,\tau] = \sigma$. Entonces,

$$E_m(\sigma,\tau) = [...[\sigma,\overbrace{\tau],\tau],...,\tau}^{m}] = \sigma.$$

□

Además, en demostración del lema 2.1.5, se puede observar que si no exigimos que $\tau \in A_n$, entonces para todo ciclo de longitud $r > 3$, $\sigma \in A_n$, existe $\tau \in S_n$ con $sop(\tau) \subset sop(\sigma)$ y $E_m(\sigma,\tau) = \sigma$ para todo $m \in \mathbb{N}$.

El siguiente resultado generaliza el lema 2.1.6 para palabras de Engel de longitud arbitraria.

Lema 2.2.5. *Todo ciclo σ de longitud impar $n \geq 5$ se puede escribir como un producto de dos palabras de Engel de longitud m en A_n.*

Demostración. Sea $\sigma = (1,...,n)$. Se puede expresar σ como $\sigma_1\sigma_2$ con $\sigma_1 = (1,2,3)$ y $\sigma_2 = (3,4,5,...,n)$. Hemos demostrado en el lema 2.1.6 que existen $\zeta_1, \zeta_2 \in A_n$ tales que $\sigma_i = E_2(\sigma_i,\zeta_i)$ con $i \in \{1,2\}$. Entonces $\sigma_i = E_m(\sigma_i,\zeta_i)$ para una longitud arbitraria m y

$$\sigma = E_m(\sigma_1,\zeta_1)E_m(\sigma_2,\zeta_2).$$

□

Extenderemos ahora el lema 2.1.7 a palabras de Engel de longitud arbitraria. Es decir, estudiaremos el caso en que los ciclos involucrados en una permutación $\sigma \in A_n$ tienen longitud 3.

Lema 2.2.6. *Sea σ una permutación par en A_n que se puede expresar como producto de 3-ciclos disjuntos con al menos dos factores. Entonces para todo $m \geq 2$, σ es un producto de dos palabras de Engel de longitud m in A_n, con $n = sop(\sigma)$.*

Demostración. Como en el lema 2.1.7, es suficiente realizar la prueba cuando σ es un producto de dos o de tres 3-ciclos. En la demostración del lema 2.1.7, obtuvimos que

$$E_2((a,b,c)(d,e,f),(a,b)(d,e)) = (a,b,c)(d,e,f),$$
$$E_2((g,h,i),(g,h)(a,b)) = (g,h,i).$$

De este modo tendremos

$$(a,b,c)(d,e,f) = E_m((a,b,c)(d,e,f),(a,b)(d,e)),$$
$$(g,h,i) = E_m((g,h,i),(g,h)(a,b)).$$

Una aplicación directa del corolario 2.2.2 termina la demostración. □

Este último resultado asegura que si $\sigma \in A_m$, $m \geq 5$, es una permutación que se puede escribir como producto de ciclos de longitud impar disjuntos, siendo el número de $3-$ciclos distinto de 1 (esto es, permutaciones de tipo (I) o (II)), σ es un producto de dos palabras de Engel de longitud arbitraria.

Lema 2.2.7. *Sea σ una permutación en A_n, $n = sop(\sigma)$, que se expresa como un producto de dos ciclos disjuntos de longitud par, entonces para todo $m \in \mathbb{N}$, σ es un producto de dos palabras de Engel de longitud m en A_n.*

Demostración. La demostración es totalmente análoga a la que se realizó en el lema 2.1.9. □

Resuelto el caso de las permutaciones de tipo (III), sólo necesitamos estudiar las permutaciones de tipo (IV).

Lema 2.2.8. *Sea σ una permutación de tipo (IV) en A_n. Entonces para todo $m \in \mathbb{N}$, σ es un producto de dos palabras de Engel de longitud m en A_n.*

Demostración. La demostración de este resultado repite los argumentos usados para probar el lema 2.1.10. □

Con todos los resultados previos, hemos probado el teorema análogo a 2.1.11 para el caso de palabras de Engel de longitud arbitraria:

Teorema 2.2.9. *Toda permutación en A_n se puede escribir como un producto de dos palabras de Engel de longitud arbitraria en A_n.*

El teorema anterior se puede extender al siguiente corolario:

Corolario 2.2.10. *Dados dos enteros positivos m_1 y m_2, toda permutación en A_n se puede escribir como producto de dos palabras de Engel de longitudes m_1 y m_2 respectivamente en A_n.*

Demostración. Supongamos, sin pérdida de generalidad, que $m_1 \geq m_2$. Aplicando el teorema 2.2.9 sobre m_1 obtenemos que

$$A_n = E_{m_1}(A_n)E_{m_1}(A_n).$$

Como para todo $r > k$, se tiene que $E_r(A_n) \subset E_k(A_n)$, tendremos que

$$A_n = E_{m_1}(A_n)E_{m_1}(A_n) \subset E_{m_1}(A_n)E_{m_2}(A_n) \subset A_n.$$

□

Capítulo 3

Palabras de Engel de longitud 2

En el capítulo anterior hemos probado que todo elemento de un grupo Alternado A_n, con $n \geq 5$, es un producto de, a lo sumo, dos palabras de Engel de longitud arbitraria. Ahora abordaremos el problema central de esta tesis, probar que un elemento arbitrario de un grupo alternado de grado mayor o igual que 5 es una palabra de Engel de longitud arbitraria m en dicho grupo alternado. En este capítulo probaremos el resultado cuando la longitud m es 2.

En primer lugar, se probará que todo elemento de un grupo alternado que sea un producto de ciclos disjuntos de longitud impar se puede escribir como una palabra de Engel de longitud 2 en A_n. Posteriormente, probaremos el mismo resultado cuando tratemos con productos de un número par de ciclos de longitud par. Y por último, se probará que todo elemento de un grupo alternado es una palabra de Engel de longitud 2.

Recordemos que en el capítulo anterior hemos probado que algunos elementos se pueden escribir como una palabra de Engel de longitud arbitraria.

En todo el capítulo el grado del grupo Alternado A_n, n, es entero mayor o igual que 5.

Recordemos dos hechos ampliamente utilizados en lo que sigue y que ya se han probado en el texto.

1. Si $\sigma := (a, b, c)$, $\sigma = E_m((a, b, c), (a, b)) = E_2((a, b), (a, c)) \in E_m(S_3)$, para todo $m \in \mathbb{N}$.

2. Si $\sigma := (a, b)(c, d)$, sabemos que $\sigma \in E_m(A_n)$, para todo $m \in \mathbb{N}$ (lema 2.2.3).

Dado que A_3 es abeliano, es claro que (a, b, c) no puede expresarse como una palabra de Engel de longitud m de dos elementos de A_3. Pero $(a, b, c) = E_m((a, b, c), (a, b)(d, e)) \in E_m(A_5)$.

Este hecho jugará un papel importante importante en las demostraciones de este capítulo.

Observemos que un 3-ciclo se puede expresar como una palabra de Engel, de cualquier longitud, en S_3 en la que el primer elemento puede ser par o impar, pero el segundo elemento es siempre impar. No puede expresarse como una palabra de Engel en S_3 en que la segunda permutación sea par.

Si bien se ha probado que si $n \geq 5$ y σ es un ciclo en A_n de longitud r, con $5 \leq r \leq n-2$, se tiene que $\sigma \in E_m(A_n)$, para todo $m \in \mathbb{N}$ (véase el lema 2.2.4), este resultado no permite el uso del lema 2.1.1 al considerar una permutación par expresada como producto de ciclos disjuntos.

Para poder aplicar el lema 2.1.1 a un elemento $\sigma \in A_n$, necesitamos tener una descomposición de σ en producto de permutaciones disjuntas σ_i de modo que cada factor $\sigma_i \in E_2(A_{sop(\sigma_i)})$.

Por tanto, en el párrafo siguiente n representará siempre un entero mayor o igual que 5 y los ciclos considerados serán de longitud n.

3.1. Ciclos de longitud impar

En este apartado consideraremos ciclos de longitud impar. El objetivo es probar que dado un ciclo σ de longitud n impar mayor o igual que 5, se puede escribir como una palabra de Engel de longitud 2 en A_n.

El lema siguiente ya ha sido mencionado para los ciclos de longitud 3, pero es válido para cualquier ciclo de longitud impar.

Lema 3.1.1. *Todo ciclo σ de longitud impar n es una palabra de Engel de longitud 2 en S_n.*

Demostración. Sea σ un ciclo de longitud n en A_n. Basta con observar que σ^2 es un elemento de $Cl_{S_n}(\sigma)$, y por tanto existe y en S_n verificando que $\sigma^y = \sigma^2$. Por lo tanto, $[\sigma, y] = \sigma$ y $E_2(\sigma, y) = \sigma$. De hecho,

$$\sigma = E_2(\sigma, y), \quad \text{para todo} \quad m \geq 2.$$

□

Lema 3.1.2. *Supongamos que n es impar y no es múltiplo de 3. Si σ es un ciclo de longitud n en A_n existen permutaciones $\xi, \tau \in A_n$ tales que $\sigma = E_2(\xi, \tau)$.*

Demostración. Por 2.1.3 basta probar que existe un n-ciclo que es una palabra de Engel de longitud 2 en A_n. Dado un n-ciclo σ, σ, σ^{-1} y σ^2 son permutaciones del mismo tipo. Luego dos de ellas estarán en la misma clase de conjugación en A_n. Tenemos así tres posibilidades:

1. Si σ^{-1} es un elemento de $Cl_{A_n}(\sigma)$, se tiene que existe una permutación y en A_n verificando que $(\sigma^{-1})^y = \sigma$, de donde se deduce que $[\sigma^{-1}, y] = \sigma^2$, y por tanto que $E_2(\sigma^{-1}, y) = \sigma^{-4}$ que es un n-ciclo.

2. Si σ^2 es un elemento de $Cl_{A_n}(\sigma)$, existe y en A_n verificando que $\sigma^y = \sigma^2$. Por tanto $[\sigma, y] = \sigma$ y $E_2(\sigma, y) = \sigma$.

3. Si σ^{-1} es un elemento de $Cl_{A_n}(\sigma^2)$, luego existe y en A_n, tal que $(\sigma^{-1})^y = \sigma^2$, lo que implica que $[\sigma, y] = \sigma^{-3}$ y $E_2(\sigma, y) = \sigma^9$.

   Como $mcd(9, n) = 1$, por hipótesis, se tiene que σ^9 será un n-ciclo.

□

Consideraremos por separado los casos $n \equiv 1$ y $n \equiv 3$ *mod* (4).

Lema 3.1.3. *Consideremos $n \equiv 1$ mod 4 y sea σ un ciclo de longitud n en A_n. Entonces σ se puede escribir como una palabra de Engel de longitud 2 en A_n.*

Demostración. Consideremos $\sigma = (1, 2, 3..., n)$ en A_n. Como por hipótesis tenemos que $n \equiv 1$ *mod* 4, tendremos que $n-1 \equiv 0$ *mod* 4, es decir, $n = 1+4r$ para algún $r \geq 1$.

De este modo, si tomamos

$$\tau := (2, n)(3, n-1)(4, n-2)...(2r+1, 2r+2),$$

tendremos que τ es una permutación en A_n, pues es un producto de $2r$ transposiciones.

Se tiene que $\sigma^\tau = \sigma^{-1}$, luego $[\sigma, \tau] = \sigma^{-2}$. Por tanto

$$\sigma^4 = E_2(\sigma, \tau) \in E_2(A_n).$$

Como $mcd(4, n) = 1$, se tiene que σ^4 es un ciclo de longitud n en A_n. Basta aplicar el lema 2.1.3 para obtener el resultado. □

Así, sólo queda ver qué ocurre cuando $r \equiv 3$ *mod* 4.

Lema 3.1.4. *Sea $n \equiv 3$ mod 4 y $\sigma \in A_n$ un ciclo de longitud n. Entonces σ es una palabra de Engel de longitud 2 en A_n.*

Demostración. Si $n = 7$ o $n = 11$, podemos aplicar el lema 3.1.2 para obtener el resultado.

Si $n = 15$, consideremos las siguientes permutaciones en A_{15}:

$$\begin{aligned} \xi &= (1, 14, 12, 10, 8, 6, 2, 5, 7, 9, 11, 13, 15), \\ \tau &= (2, 3)(4, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5). \end{aligned}$$

Conmutemos ahora ξ y τ

$$\begin{aligned} \zeta &= [\xi, \tau] = \xi^{-1}\tau^{-1}\xi\tau \\ &= (1, 15, 13, 11, 9, 7, 5, 2, 6, 8, 10, 12, 14) \\ &\quad (2, 3)(4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) \\ &\quad (1, 14, 12, 10, 8, 6, 2, 5, 7, 9, 11, 13, 15) \\ &\quad (2, 3)(4, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5) \\ &= (1, 13, 9, 5, 2, 6, 10, 14, 4, 15, 11, 7, 3, 8, 12). \end{aligned}$$

Conmutando otra vez por τ tendremos que

$$\begin{aligned} \sigma &= [\zeta, \tau] = \zeta^{-1}\tau^{-1}\zeta\tau \\ &= (1, 12, 8, 3, 7, 11, 15, 4, 14, 10, 6, 2, 5, 9, 13) \\ &\quad (2, 3)(4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) \\ &\quad (1, 13, 9, 5, 2, 6, 10, 14, 4, 15, 11, 7, 3, 8, 12) \\ &\quad (2, 3)(4, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5) \\ &= (1, 10, 2, 13, 12, 3, 11, 4, 8, 5, 14, 6, 7, 15, 9). \end{aligned}$$

De este modo, $E_2(\xi, \tau)$ es un 15-ciclo. Basta con aplicar el lema 2.1.1 para extender el resultado a todo elemento de $Cl_{S_{15}}(\sigma)$.

Si $n > 15$, gracias al lema 3.1.2 basta considerar los casos en los que n es un múltiplo de 3, por lo tanto, podemos suponer que $n \geq 27$. Vamos a considerar las siguientes permutaciones:

$$\begin{aligned} \xi &= (1, n-1, n-3, n-5, ..., 8, 6, 2, 5, 7, 9, ..., n-4, n-2, n), \\ \tau &= (2, 3)(4, n, n-1, n-2, ..., 6, 5). \end{aligned}$$

Observemos que ξ es un ciclo de longitud $n-2$, cuyo soporte es $sop(\xi) = \{1, ..., n\}\backslash\{3, 4\}$, y que τ es un producto de dos ciclos de longitud par, el primero de longitud 2 y el segundo de longitud $n-3$. El $sop(\tau) = \{2, 3, ..., n\}$.

Conmutemos ahora ξ y τ. Si ζ denota el conmutador de estos elementos, tenemos que

$$\begin{aligned}
\zeta &= [\xi,\tau] = \xi^{-1}\tau^{-1}\xi\tau \\
&= \{(1,n,n-2,n-4,...,7,5,2,6,8,...,n-5,n-3,n-1)\} \\
&\quad \{(2,3)(4,5,6,...,n-2,n-1,n)\} \\
&\quad \{(1,n-1,n-3,n-5,...,8,6,2,5,7,...,n-4,n-2,n)\} \\
&\quad \{(2,3)(4,n,n-1,n-2,...,6,5)\} \\
&= (1,n-2,n-6,n-10,...,13,9,5,2,6,10,14,18,... \\
&\quad ...,n-1,4,n,n-4,n-8,...,15,11,7,3,8,12,... \\
&\quad ...,n-11,n-7,n-3).
\end{aligned}$$

Vemos que que ζ es un n-ciclo. Al conmutar de nuevo ζ y τ, obtenemos que

$$\begin{aligned}
\lambda &= [\zeta,\tau] = \zeta^{-1}\tau^{-1}\zeta\tau \\
&= \{(1,n-3,n-7,n-11,...,16,12,8,3,7,11,15,... \\
&\quad ...,n-8,n-4,n,4,n-1,n-5,n-9,n-13,... \\
&\quad ...,14,10,6,2,5,9,..,n-10,n-6,n-2)\} \\
&\quad \{(2,3)(4,5,6,...,n-2,n-1,n)\} \\
&\quad \{(1,n-2,n-6,n-10,...,13,9,5,2,6,10,14,18,... \\
&\quad ...,n-1,4,n,n-4,n-8,...,15,11,7,3,8,12,... \\
&\quad ...,n-11,n-7,n-3\}) \\
&\quad \{(2,3)(4,n,n-1,n-2,...,6,5)\} \\
&= (1,n-5,n-13,n-21,...,18,10,2,13,21,29,... \\
&\quad ...,n-18,n-10,n-2,n-3,n-11,n-19,...,20,12,3, \\
&\quad 11,19,...,n-12,n-4,4,n-7,n-15,...,16,8,5, \\
&\quad n-1,n-9,n-17,...,14,6,7,15,23,...,n-16,n-8, \\
&\quad n,9,17,...,n-22,n-14,n-6).
\end{aligned}$$

Vemos que λ es un n-ciclo. Por tanto hemos encontrado un n-ciclo que verifica que

$$\lambda = E_2(\xi,\tau) \in E_2(A_n).$$

Basta aplicar ahora el lema 2.1.3 para obtener el resultado. □

3.2. Producto de ciclos de longitud impar

Una vez estudiados los ciclos de longitud impar, vamos a considerar productos de ellos.

Es evidente que si σ es una permutación par que es producto de ciclos disjuntos de longitud impar mayor que 3, los lemas 3.1.3, 3.1.4 y 2.1.1 nos aseguran el siguiente resultado.

Corolario 3.2.1. *Sea $\sigma \in A_n$ una permutación que es producto de ciclos disjuntos, cada uno de longitud impar y mayor que 3. Entonces, σ es una palabra de Engel de longitud 2 en $A_{sop(\sigma)}$ y por lo tanto, en A_n.*

Falta considerar los 3-ciclos. Como ya se ha hecho notar anteriormente es imposible escribir un 3-ciclo como una palabra de Engel de longitud 2 en A_3, por lo tanto tienen que ser considerados de forma independiente.

Lema 3.2.2. *Sea σ una permutación en A_n que puede ser escrita como producto de dos o más 3-ciclos disjuntos. Entonces, σ es una palabra de Engel de longitud 2 en $A_{sop(\sigma)}$, y, por lo tanto en A_n.*

Demostración. Consideremos $\sigma := \tau_1 ... \tau_r$, con $r \geq 2$ y τ_i un 3-ciclo para todo $i \in \{1, 2, ..., r\}$. Es suficiente probar el resultado para $r = 2$ y para $r = 3$, pues si $r \geq 4$ bastaría agrupar los 3-ciclos haciendo subproductos de dos ó de tres de ellos y aplicar el lema 2.1.1 para resolver el problema.

1. Supongamos que $\sigma = (1, 2, 3)(4, 5, 6)$. Entonces se tiene que

$$\sigma = E_2((1, 2, 3)(4, 5, 6), (1, 2)(4, 5)) \in E_2(A_6).$$

2. En caso de que σ sea un producto de tres 3-ciclos, podemos tomar $\tau := (1, 7, 4)(2, 8, 5)(3, 9, 6)$ y $\zeta := (1, 4, 8, 2, 5, 9, 3, 6, 7)$ tendremos que

$$E_2(\tau, \zeta) = (1, 2, 3)(4, 5, 6)(7, 8, 9),$$

que es un producto de tres 3-ciclos.

Basta aplicar ahora el lema 2.1.3. □

De acuerdo con los resultados probados, si $\sigma \in A_n$ es un producto de ciclos disjuntos de longitud impar y ó bien todos ellos tienen longitud mayor o igual que 5 ó bien hay al menos dos 3-ciclos en dicho producto, entonces σ es una palabra de Engel de longitud 2 en A_n.

El problema se tiene cuando aparece exactamente un ciclo de longitud 3 y varios de longitud mayor o igual que 5.

Si conseguimos demostrar que un ciclo σ de longitud impar $n \geq 5$ se puede expresar como $\sigma = E_2(\alpha, \beta)$, con $\alpha \in A_n$ y $\beta \in S_n$ impar, podremos agrupar el 3-ciclo γ y el ciclo $\sigma = E_2(\alpha, \beta)$.

Sabemos que $\gamma = E_2(a, b)$ con $a \in A_3$ y $b \in S_3$ impar. Por lo tanto, gracias al lema 2.1.1 tendremos que

$$\gamma\sigma = E_2(a\alpha, b\beta) \in E_2(A_n).$$

Veremos por tanto que todo $\sigma \in A_n$ ciclo de longitud impar se puede expresar como un conmutador $\sigma = [x, \theta]$ de modo que x sea una permutación par y θ impar.

Lema 3.2.3. *Sea $n \geq 2$. Tomemos σ en A_{2n+1} un ciclo de longitud $2n+1$. Entonces, existen x en A_{2n+1} y θ en $S_{2n+1}\backslash A_{2n+1}$ tales que $\sigma = [x, \theta]$.*

Demostración. Consideremos las siguientes permutaciones:

$$\xi = (1, 2, 3, 4, ..., 2n-1, 2n, 2n+1) \in A_{2n+1}$$

$$\tau = (2, 4, 6, ..., 2n-2, 2n, 2n+1, 2n-1, ..., 7, 5, 3) \in S_{2n+1}\backslash A_{2n+1},$$

pues es un ciclo de longitud $2n$.

Nos encontramos con dos casos que conviene separar para poder operar correctamente:

1. Si n es par, tendremos que:

$$\begin{aligned}[\xi, \tau] &= (1, 2n+1, 2n, ..., 5, 4, 3, 2) \\ &\quad (2, 3, 5, ..., 2n-1, 2n+1, 2n, 2n-2, ..., 8, 6, 4) \\ &\quad (1, 2, 3, 4, ..., 2n-1, 2n, 2n+1) \\ &\quad (2, 4, 6, ..., 2n-2, 2n, 2n+1, 2n-1, ..., 7, 5, 3) \\ &= (1, 2, 6, 10, ..., 2n-6, 2n-2, 2n-1, 2n-5, ..., 11, 7, \\ &\quad 3, 4, 8, 12, ..., 2n-8, 2n-4, 2n, 2n+1, 2n-3, 2n-7, ..., \\ &\quad ..., 13, 9, 5).\end{aligned}$$

2. Si n es impar, tendremos que:

$$\begin{aligned}[\xi, \tau] &= (1, 2n+1, 2n, ..., 5, 4, 3, 2) \\ &\quad (2, 3, 5, ..., 2n-1, 2n+1, 2n, 2n-2, ..., 8, 6, 4) \\ &\quad (1, 2, 3, 4, ..., 2n-1, 2n, 2n+1) \\ &\quad (2, 4, 6, ..., 2n-2, 2n, 2n+1, 2n-1, ..., 7, 5, 3) \\ &= (1, 2, 6, 10, ..., 2n-8, 2n-4, 2n, 2n+1, 2n-3, 2n-7, ..., \\ &\quad ..., 11, 7, 3, 4, 8, 12, ..., 2n-6, 2n-2, 2n-1, 2n-5, ..., \\ &\quad ..., 13, 9, 5).\end{aligned}$$

En ambos casos obtenemos un ciclo de longitud $2n+1$. Basta ahora con aplicar el lema 2.1.3 para obtener el resultado. □

Ahora probaremos que dado σ un ciclo de longitud máxima en A_n, podemos encontrar permutaciones x en A_{2n+1} y θ en $S_{2n+1}\backslash A_{2n+1}$ tales que $\sigma = E_2(x,\theta)$.

Lema 3.2.4. *Sea $n \geq 2$ y $\sigma \in A_{2n+1}$ un ciclo de longitud $2n+1$. Entonces, existen elementos $x \in A_{2n+1}$ y $\theta \in S_{2n+1}\backslash A_{2n+1}$ tales que $\sigma = E_2(x,\theta)$.*

Demostración. Gracias al lema 2.1.3, es suficiente probarlo para

$$\xi = (1,2,3...,2n+1) \in A_{2n+1}.$$

Por el lema 3.2.3, sabemos que existe z en S_{2n+1}, verificando que

$$\xi = [\xi,\tau]^z = [\xi^z,\tau^z],$$

siendo τ, como en el lema 3.2.3,

$$\tau \;=\; (2,4,6,...,2n-2,2n,2n+1,2n-1,...,7,5,3) \in S_{2n+1}\backslash A_{2n+1}.$$

El objetivo ahora será intentar escribir ξ^z como un conmutador de la forma $[a,\tau^z]$, con a en A_{2n+1}, para así obtener que

$$\xi = [\xi^z,\tau^z] = [[a,\tau^z],\tau^z] = E_2(a,\tau^z) \in E_2(A_{2n+1}, S_{2n+1}\backslash A_{2n+1}).$$

Considerando $Cl_{A_{2n+1}}(\xi)$, la clase de conjugación de ξ en A_{2n+1}, tenemos que

$$\begin{array}{ccccc} \xi^z = [a,\tau^z], a \in A_{2n+1} & \iff & \xi^z(\tau^z)^{-1} \in Cl_{A_{2n+1}}((\tau^z)^{-1}) & \iff \\ (\xi\tau^{-1})^z \in Cl_{A_{2n+1}}((\tau^z)^{-1}) & \iff^{(1)} & \xi\tau^{-1} \in Cl_{A_{2n+1}}(\tau^{-1}) & \end{array}$$

Demostremos (1), pues es la única implicación que no es obvia.

1. Supongamos que $(\xi\tau^{-1})^z \in Cl_{A_{2n+1}}((\tau^z)^{-1})$. Entonces existe β en A_{2n+1} verificando que $((\xi\tau^{-1})^z)^\beta = (\tau^z)^{-1}$. Entonces, se tiene que

$$((\xi\tau^{-1}))^{\beta^{z^{-1}}} = \tau^{-1} \quad \text{y} \quad \beta^{z^{-1}} \in A_{2n+1}.$$

   Así, tendremos que $\xi\tau^{-1} \in Cl_{A_{2n+1}}(\tau^{-1})$.

2. Supongamos ahora que $\xi\tau^{-1} \in Cl_{A_{2n+1}}(\tau^{-1})$. Entonces existe β en A_{2n+1} verificando que $(\xi\tau^{-1})^{\beta} = \tau^{-1}$. Entonces, se tiene que

$$\tau^{-1} = (\xi\tau^{-1})^{\beta} = (\xi\tau^{-1})^{(zz^{-1})\beta},$$

de donde se obtiene que:

$$(\tau^{-1})^{z} = (\xi\tau^{-1})^{(zz^{-1})\beta z} = ((\xi\tau^{-1})^{z})^{\beta z},$$

y por tanto

$$((\xi\tau^{-1})^{z}) \in Cl_{A_{2n+1}}((\tau^{-1})^{z})$$

Calculemos explícitamente el producto $\xi\tau^{-1}$.

$$\begin{aligned} \xi\tau^{-1} &= (1,2,3,4,...,2n-1,2n,2n+1) \\ &\quad (2,3,5,7,...,2n-1,2n+1,2n,2n-2,...,8,6,4) \\ &= (1,2,4,3,6,5,...,2n-3,2n,2n-1). \end{aligned}$$

Como $\xi\tau^{-1}$ es un $2n$-ciclo en S_{2n+1}, es también un elemento de $Cl_{S_{2n+1}}(\tau^{-1})$.

Sabemos que existe β en S_{2n+1} verificando que $(\xi\tau^{-1})^{\beta} = \tau^{-1}$. Tomando $a = \beta$ si β es una permutación par y $a = \beta\tau$ si β es impar, tendremos que $a \in A_{2n+1}$ y

$$\xi = E_2(a, \tau^{z}).$$

□

Una vez demostrados estos dos últimos resultados, es posible enunciar y demostrar el teorema principal de esta sección.

Teorema 3.2.5. *Sea σ una permutación en A_n que se puede escribir como producto de ciclos disjuntos de longitud impar. Entonces σ es una palabra de Engel de longitud 2 en A_n. Salvo en el caso en el que σ es un 3-ciclo, σ es, de hecho, una palabra de Engel de longitud 2 en $A_{sop(\sigma)}$.*

Demostración. Supongamos que $\sigma = \tau_1...\tau_k\eta_1...\eta_r$, con τ_i un 3-ciclo para todo i en $\{1,...,k\}$ y η_j un ciclo de longitud impar y mayor que 3 para todo j en $\{1,...,r\}$.

Como se ha indicado, el único caso que presenta problemas corresponde a $k = 1$ y $r > 0$. En vista de los lemas 3.1.3 y 3.1.4, se tiene que para cada $i \in \{2,...,r\}$ existen permutaciones α_i, β_i en $A_{sop(\tau_i)}$ tales que $\eta_i = E_2(\alpha_i, \tau_i)$.

Por el lema 3.2.4 sabemos que existe $\gamma_1 \in A_{sop(\eta_1)}$ y que existe $\gamma_2 \in S_{sop(\eta_1)} \backslash A_{sop(\eta_1)}$ tales que $\eta_1 = E_2(\gamma_1, \gamma_2)$. Por tanto

$$\sigma = (1,2,3)\eta_1 ... \eta_r = E_2((1,2,3),(1,2))E_2(\gamma_1,\gamma_2)E_2(\prod_{i\geq 2}\alpha_i, \prod_{i\geq 2}\beta_i),$$

de este modo, usando el lema 2.1.1 tendremos que

$$\sigma = E_2((1,2,3)\gamma_1 \prod_{i\geq 2}\alpha_i, (1,2)\gamma_2 \prod_{i\geq 2}\beta_i) \in E_2(A_{sop(\sigma)}).$$

□

3.3. Producto de ciclos de longitud par

En este párrafo estudiamos las permutaciones del grupo alternado que son producto de un número par de ciclos de longitud par. Basta probar que si σ es un producto de dos ciclos disjuntos de longitud par, se puede escribir como una palabra de Engel de longitud 2 en $A_{sop(\sigma)}$.

El lema 2.1.1 permitirá extender este resultado a un producto arbitrario de un número par de ciclos disjuntos de longitud par.

En primer lugar estudiaremos las permutaciones producto de un 2-ciclo y un $2r$-ciclo.

Lema 3.3.1. *Sea $n > 2$. Toda permutación ζ que sea producto de un 2-ciclo y un $(2n-2)$-ciclo disjuntos es una palabra de Engel de longitud 2 de la forma $E_2(\alpha, \beta)$, con $\alpha \in S_{2n}$ y $\beta \in A_{2n}$.*

Demostración. Consideremos las siguientes permutaciones

$$\tau = (1,2n)(2,3)(4,5)...(2n-4,2n-3) \in S_{2n}$$

$$\xi = (1,2n-1,2n-2,2n-3...,4,3,2) \in A_{2n}.$$

Notar que τ es un producto de $n-1$ trasposiciones disjuntas y que $2n-2$, $2n-1$ no pertenecen a $sop(\tau)$. ξ es un ciclo de longitud $2n-1$ (luego es una permutación par) y $2n \notin sop(\xi)$.

Calcularemos $[\tau, \xi]$ en primer lugar:

$$\begin{aligned}\sigma &= [\tau,\xi] = \tau^{-1}\xi^{-1}\tau\xi \\ &= \{(1,2n)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-3)\} \\ &\quad \{(1,2,3,4,...,2n-3,2n-2,2n-1)\} \\ &\quad \{(1,2n)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-3)\} \\ &\quad \{(1,2n-1,2n-2,2n-3,...,4,3,2)\} \\ &= (1,2n,3,5,7,9,...,2n-7,2n-5,2n-3, \\ &\quad 2n-2,2n-4,2n-6,...,8,6,4,2).\end{aligned}$$

Es claro que σ es un ciclo de longitud impar $2n-1$. (Notar que σ fija a la cifra $2n-1$).

Consideremos ahora,

$$\begin{aligned}E_2(\tau,\xi) &= [\sigma,\xi] = \sigma^{-1}\xi^{-1}\sigma\xi \\ &= \{(1,2,4,6,8,...,2n-6,2n-4,2n-2, \\ &\quad 2n-3,2n-5,2n-7,...,9,7,5,3,2n)\} \\ &\quad \{(1,2,3,4,...,2n-3,2n-2,2n-1)\} \\ &\quad \{(1,2n,3,5,7,9,...,2n-7,2n-5,2n-3, \\ &\quad 2n-2,2n-4,2n-6,...,8,6,4,2)\} \\ &\quad \{(1,2n-1,2n-2,2n-3,...,4,3,2)\}\end{aligned}$$

Vamos a separar dos casos:

1. Si n es par, tendremos que

$$\begin{aligned}[\sigma,\xi] &= (1,2)(3,4,8,12,16,...,2n-8,2n-4, \\ &\quad 2n-3,2n-7,2n-11,...,17,13,9,5, \\ &\quad 2n,6,10,...,2n-10,2n-6,2n-2, \\ &\quad 2n-1,2n-5,2n-9,...,15,11,7).\end{aligned}$$

2. Si n es impar, tendremos que

$$\begin{aligned}[\sigma,\xi] &= (1,2)(3,4,8,12,16,...,2n-6,2n-2, \\ &\quad 2n-1,2n-5,2n-9,...,17,13,9,5, \\ &\quad 2n,6,10,...,2n-12,2n-8,2n-4, \\ &\quad 2n-3,2n-7,2n-11,...,15,11,7).\end{aligned}$$

En ambos casos, se puede observar que $[\sigma,\xi]$ es un producto de un 2-ciclo por un $(2n-2)$-ciclo.

Basta aplicar el lema 2.1.3 para extender el resultado a todo elemento del mismo tipo. □

Es importante notar que las permutaciones aparecen en la palabra de Engel no son siempre permutaciones pares.

Como τ es un producto de $n-1$ trasposiciones disjuntas, si n es un número impar τ será un elemento de A_{2n} y por lo tanto, todo producto de un 2-ciclo y un $(2n-2)$-ciclo disjuntos en A_{2n} es una palabra de Engel de longitud 2 en A_{2n}.

Todo esto se recoge en el siguiente corolario.

Corolario 3.3.2. *Sea $n > 2$ e impar. Toda permutación que pueda escribirse como producto de un 2-ciclo y un $(2n-2)$-ciclo disjuntos en A_{2n} es una palabra de Engel de longitud 2 en A_{2n}.*

Queda estudiar el caso en el que n es un número par que trataremos en el siguiente resultado.

Lema 3.3.3. *Sea $n > 2$ par. Consideremos σ una permutación que es un producto disjunto de un 2-ciclo y un $(2n-2)$-ciclo. Entonces σ es una palabra de Engel de longitud 2 en A_{2n}.*

Demostración. Consideremos las permutaciones siguientes:

$$\begin{aligned} \xi &= (1,2n)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-2,2n-1), \\ \tau &= (2,3,4,...,2n-3,2n-2,2n-1,2n), \end{aligned}$$

que son ambas permutaciones en A_{2n}. En primer lugar, calcularemos el conmutador de ξ y τ:

$$\begin{aligned} \lambda &= [\xi,\tau] = \xi^{-1}\tau^{-1}\xi\tau \\ &= \{(1,2n)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-1,2n-2)\} \\ &\quad \{(2,2n,2n-1,2n-2,2n-3,...,5,4,3)\} \\ &\quad \{(1,2n)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-2,2n-1)\} \\ &\quad \{(2,3,4,...,2n-3,2n-2,2n-1,2n)\} \\ &= (1,2n-2,2n-6,2n-8,2n-10,...,8,6,4,2) \\ &\quad (3,5,7,...,2n-5,2n-3,2n-4,2n-1,2n). \end{aligned}$$

Es claro que λ es producto dos ciclos de longitudes $n-1$ y $n+1$ respectivamente.

Conmutemos de nuevo por τ para obtener el resultado deseado.

$$\begin{aligned} E_2(\xi,\tau) &= [\lambda,\tau] = \lambda^{-1}\tau^{-1}\lambda\tau \\ &= \{(1,2,4,6,...,2n-8,2n-6,2n-2) \\ &\quad (3,2n,2n-1,2n-4,2n-3,2n-5,2n-7,...,9,7,5)\} \\ &\quad \{(2,2n,2n-1,2n-2,2n-3,...,5,4,3)\} \\ &\quad \{(1,2n-2,2n-6,2n-8,2n-10,...,8,6,4,2) \\ &\quad (3,5,7,...,2n-5,2n-3,2n-4,2n-1,2n)\} \\ &\quad \{(2,3,4,...,2n-3,2n-2,2n-1,2n)\} \\ \\ &= (1,2n-5)(2,6,10,...,2n-10,2n-6,2n-3,2n-9,2n-13,..., \\ &\quad ...,11,7,3,2n-1,4,8,...,2n-8,2n-2,2n-4,2n-7,2n-11,..., \\ &\quad ...,13,9,5,2n). \end{aligned}$$

Denotemos por μ a la permutación anterior. Se observa que $sop(\mu) = \{1,...,2n\}$ y que μ es un producto disjunto de un 2-ciclo y un $(n-2)$-ciclo. Basta aplicar el lema 2.1.3 para obtener el resultado.

□

A continuación estudiaremos el caso en el que n es par, y la permutación $\sigma \in A_{2n}$ es un producto de dos ciclos disjuntos de longitud n.

Lema 3.3.4. *Sea $n > 2$ par. Consideremos σ una permutación en A_{2n} que es un producto de dos n-ciclos disjuntos. Entonces σ es una palabra de Engel de longitud 2 en A_{2n}.*

Demostración. Consideraremos las siguientes permutaciones en A_{2n}:

$$\xi = (2n,1)(2,3)(4,5)...(2n-6,2n-5)(2n-4,2n-3)(2n-2,2n-1),$$

$$\tau = (1,2,3,...,2n-2,2n-1).$$

Calculemos primero el conmutador de ξ y τ:

$$\begin{aligned} \mu &= [\xi,\tau] = \xi^{-1}\tau^{-1}\xi\tau \\ &= \{(2n,1)(2,3)...(2n-6,2n-5)(2n-4,2n-3)(2n-2,2n-1)\} \\ &\quad \{(1,2n-1,2n-2,...,4,3,2)\} \\ &\quad \{(2n,1)(2,3)...(2n-6,2n-5)(2n-4,2n-3)(2n-2,2n-1)\} \\ &\quad \{(1,2,3,...,2n-2,2n-1)\} \\ \\ &= (1,3,5,7,9,...,2n-5,2n-3,2n-1) \\ &\quad (2,2n,2n-2,2n-4,...,10,8,6,4). \end{aligned}$$

Se observa que $sop(\mu) = \{1, 2, 3, ..., 2n\}$ y que μ es pruducto de dos ciclos disjuntos de longitud n.

Conmutemos de nuevo por τ para obtener:

$$\begin{aligned} E_2(\xi, \tau) &= [\mu, \tau] = \mu^{-1}\tau^{-1}\mu\tau \\ &= \{(1, 2n-1, 2n-3, 2n-5, ..., 9, 7, 5, 3) \\ &\quad (2, 4, 6, 8, 10, ..., 2n-4, 2n-2, 2n)\} \\ &\quad \{(1, 2n-1, 2n-2, ..., 4, 3, 2)\} \\ &\quad \{(1, 3, 5, 7, 9, ..., 2n-5, 2n-3, 2n-1) \\ &\quad (2, 2n, 2n-2, 2n-4, ..., 10, 8, 6, 4)\} \\ &\quad \{(1, 2, 3, ..., 2n-2, 2n-1)\} \\ &= (1, 2, 6, 10, ..., 2n-6, 2n-2, 2n-3, 2n-7, ..., 13, 9, 5) \\ &\quad (3, 2n-1, 4, 8, 12, ..., 2n-4, 2n, 2n-5, 2n-9, ..., 11, 7). \end{aligned}$$

Vemos que $E_2(\xi, \tau)$ es producto de dos ciclos disjuntos cada uno de longitud n. Es suficiente aplicar el lema 2.1.3 para extender el resultado a todo elemento producto de dos ciclos disjuntos de longitud n. □

Ahora consideraremos permutaciones que son producto de ciclos, ambos de longitud par mayor o igual que 4.

Lema 3.3.5. *Sea $n > 2$. Toda permutación que sea un producto de un $2i$-ciclo y un $(2n-2i)$-ciclo disjuntos en A_{2n}, $1 < i < n-1$, es una palabra de Engel de longitud 2 en S_{2n}.*

Demostración. Sin pérdida de generalidad supondremos que $2i < n$. Consideremos las permutaciones

$$\tau = (1, 2)(3, 4)...(2i-1, 2n)(2i, 2i+1)...(2n-4, 2n-3) \in S_{2n}$$

$$\xi = (1, 2n-1, 2n-2, ..., 4, 3, 2) \in A_{2n}.$$

Conviene hacer notar que $2n$ no pertenece a $sop(\xi)$, que será por tanto un ciclo de longitud $2n-1$ y que ni $2n-2$, ni $2n-1$ pertenecen a $sop(\tau)$, que está formada por un producto de $n-1$ trasposiciones disjuntas.

Notemos que en sentido estricto τ está bien definida si $i \geq 3$. Se expresa de este modo para facilitar al lector la forma de las permutaciones. Para los casos más pequeños, las permutaciones anteriores serían:

- Si $i = 2$ y $n = 5$, tendremos que $\tau = (1, 2)(3, 10)(4, 5)(6, 7)$ y $\xi = (1, 9, 8, 7, 6, 5, 4, 3, 2)$.

- Si $i = 2$ y $n = 6$, tendremos que $\tau = (1,2)(3,12)(4,5)(6,7)(8,9)$ y $\xi = (1,11,10,9,8,7,6,5,4,3,2)$.

Se tiene que:

$$\begin{aligned}
\sigma &= [\tau,\xi] = \tau^{-1}\xi^{-1}\tau\xi \\
&= \{(1,2)(3,4)...(2i-1,2n)(2i,2i+1)...(2n-4,2n-3)\} \\
&\quad \{(1,2,3,4,...,2n-3,2n-2,2n-1)\} \\
&\quad \{(1,2)(3,4)...(2i-1,2n)(2i,2i+1)...(2n-4,2n-3)\} \\
&\quad \{(1,2n-1,2n-2,2n-3,...,4,3,2)\} \\
&= (1,2,4,6,...,2i-4,2i-2,2n,2i+1,2i+3,2i+5,... \\
&\quad ...,2n-5,2n-3,2n-2,2n-4,2n-6,...,2i, \\
&\quad 2i-1,2i-3,2i-5,...,7,5,3).
\end{aligned}$$

Se observa que $sop(\sigma) = \{1,2,3,...,2n-2,2n\}$ y que por tanto σ será un ciclo de longitud $2n-1$.

Notemos que, como antes, la expresión indicada de σ tiene sentido para valores de i y n suficientemente grandes. Por ejemplo:

- Si $i = 2$ y $n = 6$, tendremos que $\sigma = (1,2,12,5,7,9,10,8,6,4,3)$.
- Si $i = 3$ y $n = 7$, tendremos que $\sigma = (1,2,4,14,7,9,11,12,10,8,6,5,3)$.
- Si $i = 2$ y $n = 7$, tendremos que $\sigma = (1,2,14,5,7,9,11,12,10,8,6,4,3)$.
- Si $i = 3$ y $n = 8$, tendremos que $\sigma = (1,2,4,16,7,9,11,13,14,12,10,8,6,5,3)$.

Conmutando de nuevo con ξ, tenemos que

$$\begin{aligned}
E_2(\tau,\xi) &= [\sigma,\xi] = \sigma^{-1}\xi^{-1}\sigma\xi \\
&= \{(1,3,5,7,...,2i-5,2i-3,2i-1,2i, \\
&\quad 2i+2,2i+4,...,2n-4,2n-2,2n-3, \\
&\quad 2n-5,...,2i+5,2i+3,2i+1,2n, \\
&\quad 2n-2,2n-4,...,8,6,4,2)\} \\
&\quad \{(1,2,3,4,...,2n-3,2n-2,2n-1)\} \\
&\quad \{(1,2,4,6,...,2n-6,2n-4,2n-2,2n, \\
&\quad 2i+1,2i+3,2i+5,...,2n-5,2n-3, \\
&\quad 2n-2,2n-4,...,2i+4,2i+2,2i, \\
&\quad 2i-1,2i-3,2i-5,...,9,5,3)\} \\
&\quad \{(1,2n-1,2n-2,2n-3,...,4,3,2)\}
\end{aligned}$$

Consideraremos cuatro casos:

1. Si n e i son números pares tendremos que,

$$\begin{aligned}[\sigma,\xi] &= (1,3,7,11,...,2i-9,2i-5,2i-1,\\ &\quad 2i-2,2i-6,...,10,6,2,5,9,...,\\ &\quad ...,2i-7,2i-3,2i,2i-4,2i-8,...\\ &\quad 12,8,4)\\ &\quad (2i+1,2i+2,2i+6,...,2n-10,\\ &\quad 2n-6,2n-2,2n-1,2n-5,2n-9,...\\ &\quad ...,2i+7,2i+3,2n,2i+4,2i+8,...\\ &\quad ...,2n-8,2n-4,2n-3,2n-7,...\\ &\quad 2n-11,...,2i+13,2i+9,2i+5).\end{aligned}$$

   - Para el caso $i=2$ y $n=6$, tendremos que

$$E_2(\tau,\xi) = (1,3,2,4)(5,6,10,11,7,12,8,9).$$

2. Si n e i son números impares tendremos que,

$$\begin{aligned}[\sigma,\xi] &= (1,3,7,11,...,2i-11,2i-7,2i-3,\\ &\quad 2i,2i-4,2i-8,...,10,6,2,5,9,...,\\ &\quad ...,2i-9,2i-5,2i-1,2i-2,2i-6,...\\ &\quad 12,8,4)\\ &\quad (2i+1,2i+2,2i+6,...,2n-10,\\ &\quad 2n-6,2n-2,2n-1,2n-5,2n-9,...\\ &\quad ...,2i+7,2i+3,2n,2i+4,2i+8,...\\ &\quad ...,2n-8,2n-4,2n-3,2n-7,\\ &\quad 2n-11,...,2i+13,2i+9,2i+5).\end{aligned}$$

   - Para el caso $i=3$ y $n=7$, tendremos que

$$E_2(\tau,\xi) = (1,3,6,2,5,4)(7,8,12,13,9,14,10,11).$$

3. Si n es un número impar e i es par tendremos que,

$$\begin{aligned}[\sigma,\xi] &= (1,3,7,11,...,2i-9,2i-5,2i-1,\\ &\quad 2i-2,2i-6,...,10,6,2,5,9,...,\\ &\quad ...,2i-7,2i-3,2i,2i-4,2i-8,...\\ &\quad 12,8,4)\\ &\quad (2i+1,2i+2,2i+6,...,2n-12,\\ &\quad 2n-8,2n-4,2n-3,2n-7,2n-11,...\\ &\quad ...,2i+7,2i+3,2n,2i+4,2i+8,...\\ &\quad ...,2n-6,2n-2,2n-1,2n-5,\\ &\quad 2n-11,...,2i+13,2i+9,2i+5).\end{aligned}$$

- Para el caso $i=2$ y $n=7$, tendremos que

$$E_2(\tau,\xi) = (1,3,2,4)(5,6,10,11,7,14,8,12,13,9).$$

4. Si n es un número par e i es impar tendremos que,

$$\begin{aligned}[\sigma,\xi] &= (1,3,7,11,...,2i-11,2i-7,2i-3,\\ &\quad 2i,2i-4,2i-8,...,10,6,2,5,9,...,\\ &\quad ...,2i-9,2i-5,2i-1,2i-2,2i-6,...\\ &\quad 12,8,4)\\ &\quad (2i+1,2i+2,2i+6,...,2n-12,\\ &\quad 2n-8,2n-4,2n-3,2n-7,2n-11,...\\ &\quad ...,2i+7,2i+3,2n,2i+4,2i+8,...\\ &\quad ...,2n-6,2n-2,2n-1,2n-5,\\ &\quad 2n-11,...,2i+13,2i+9,2i+5).\end{aligned}$$

- Para el caso $i=3$ y $n=8$, tendremos que

$$E_2(\tau,\xi) = (1,3,6,2,5,4)(7,8,12,13,9,16,10,14,15,11).$$

Notemos que $E_2(\tau,\xi) = [\sigma,\xi]$ es un $2i$-ciclo por un $(2n-2i)$-ciclo. Basta aplicar el lema 2.1.3 para extender el resultado a todo elemento producto de dos ciclos de longitud par.

□

El resultado anterior nos indica que toda permutación $\sigma \in A_{2n}$ del tipo $(1,...,2i)(2i+1,...,2n)$ se puede escribir como una palabra de Engel de longitud 2 en S_{2n}, pero las permutaciones utilizadas no son siempre pares. De hecho, se tiene el siguiente corolario:

Corolario 3.3.6. *Sea $n > 2$ impar. Toda permutación que pueda escribirse como producto de un $2i$-ciclo y un $(2n-2i)$-ciclo disjuntos en A_{2n} es una palabra de Engel de longitud 2 en A_{2n}.*

Demostración. Consideremos $\zeta = (1, ..., 2i)(2i+1, ..., 2n)$. Por el lema 3.3.5, sabemos que existen ξ y τ elementos de S_{2n} verificando que $\sigma = E_2(\tau, \xi)$. Por construcción ξ es un elemento en A_{2n}, pues es un ciclo de longitud $2n-1$.

Además τ será un producto de $n-1$ trasposiciones disjuntas y $n-1$ es par. □

Luego el problema lo plantean las permutaciones σ que son producto de dos ciclos disjuntos de longitud par mayor o igual que 4 cuando $\sharp sop(\sigma) \equiv 0 \mod(4)$.

Lema 3.3.7. *Sea $n > 2$ par. Si $\sigma \in A_{2n}$ es un producto disjunto de un $2i$-ciclo y un $(2n-2i)$-ciclo, entonces σ es una palabra de Engel de longitud 2 en A_{2n}.*

Demostración. Se puede suponer, sin pérdida de generalidad que $2 \leq i < n/2$ puesto que para $i = 1$ el resultado está probado en el lema 3.3.3, para $i = n/2$ el lema 3.3.4 resuelve el problema y para $i > n/2$ basta con intercambiar los papeles de los dos ciclos involucrados en σ. Consideremos las siguientes permutaciones en A_{2n}:

$$\begin{aligned} \xi &= (2n,1)(2,3)...(2n-6,2n-5)(2n-4,2n-2,2n-1), \\ \lambda &= (1,4i-4,4i-5,...,6,5,4,3,2), \\ \tau &= (2,3,4,...,2n-1,2n). \end{aligned}$$

Al igual que en los resultados anteriores, para valores pequeños de i y n puede no verse con claridad las permutaciones obtenidas.

Resolveremos primero el caso $n = 6$ e $i = 2$ como ejemplo. Sean

$$\begin{aligned} \xi &= (12,1)(2,3)(4,5)(6,7)(8,10,11), \\ \lambda &= (1,4,3,2), \\ \tau &= (2,3,4,5,6,7,8,9,10,11,12), \\ \xi^\lambda &= (2,12)(3,4)(1,5)(6,7)(8,10,11). \end{aligned}$$

De este modo, tendremos que

$$\begin{aligned} \zeta &= [\xi^\lambda, \tau] = (\xi^\lambda)^{-1}\tau^{-1}\xi^\lambda\tau \\ &= (2,12)(3,4)(1,5)(6,7)(8,11,10) \\ &\quad (2,12,11,10,9,8,7,6,5,4,3) \\ &\quad (2,12)(3,4)(1,5)(6,7)(8,10,11) \\ &\quad (2,3,4,5,6,7,8,9,10,11,12) \\ &= (1,3,12,10,6)(2,4,5,7,9,8,11). \end{aligned}$$

Conmutando otra vez por τ tendremos que

$$\begin{aligned} E_2(\xi^\lambda, \tau) &= [\zeta, \tau] = \zeta^{-1}\tau^{-1}\zeta\tau \\ &= (1,6,10,12,3)(2,11,8,9,7,5,4) \\ &\quad (2,12,11,10,9,8,7,6,5,4,3) \\ &\quad (1,3,12,10,6)(2,4,5,7,9,8,11) \\ &\quad (2,3,4,5,6,7,8,9,10,11,12) \\ &= (1,11,7,12)(2,8,5,6,9,4,10,3). \end{aligned}$$

Volvamos al caso general y empecemos calculando el conmutador de ξ^λ y de τ, ambas permutaciones en A_{2n}:

$$\begin{aligned} \zeta &= [\xi^\lambda, \tau] = (\xi^\lambda)^{-1}\tau^{-1}\xi^\lambda\tau \\ &= \{(1,2,3,4,...,4i-6,4i-5,4i-4)\} \\ &\quad \{(2n,1)(2,3)...(2n-6,2n-5)(2n-4,2n-1,2n-2)\} \\ &\quad \{(1,4i-4,4i-5,4i-6,...,4,3,2)\} \\ &\quad \{(2,2n,2n-1,2n-2,2n-3,...,4,3)\} \\ &\quad \{(1,2,3,4,...,4i-6,4i-5,4i-4)\} \\ &\quad \{(2n,1)(2,3)...(2n-6,2n-5)(2n-4,2n-2,2n-1)\} \\ &\quad \{(1,4i-4,4i-5,4i-6,...,4,3,2)\} \\ &\quad \{(2,3,4,...,2n-2,2n-1,2n)\} \\ &= (1,4i-5,4i-7,4i-9,...,7,5,3,2n,2n-2,2n-6, \\ &\quad 2n-8,2n-10,...,4i+4,4i+2,4i,4i-2) \\ &\quad (2,4,6,8,...,4i-6,4i-4,4i-3,4i-1,4i+1,... \\ &\quad ...,2n-7,2n-5,2n-3,2n-4,2n-1). \end{aligned}$$

Conmutaremos otra vez por τ, y tendremos en cuenta que $2n, 4i \equiv 0\ mod\ 4$.

$$\begin{aligned} E_2(\xi^\lambda, \tau) &= [\zeta, \tau] = \zeta^{-1}\tau^{-1}\zeta\tau \\ &= \{(1, 4i-2, 4i, 4i+2, 4i+4, ..., 2n-10, 2n-8, \\ &\quad 2n-6, 2n-2, 2n, 3, 5, 7, ..., 4i-9, 4i-7, 4i-5) \\ &\quad (2, 2n-1, 2n-4, 2n-3, 2n-5, 2n-7, ..., 4i+1, \\ &\quad 4i-1, 4i-3, 4i-4, 4i-6, ..., 10, 8, 6, 4)\} \\ &\quad \{(2, 2n, 2n-1, 2n-2, 2n-3, ..., 4, 3)\} \\ &\quad \{(1, 4i-5, 4i-7, 4i-9, ..., 7, 5, 3, 2n, 2n-2, 2n-6, \\ &\quad 2n-8, 2n-10, ..., 4i+4, 4i+2, 4i, 4i-2) \\ &\quad (2, 4, 6, 8, ..., 4i-6, 4i-4, 4i-3, 4i-1, 4i+1, ... \\ &\quad ..., 2n-7, 2n-5, 2n-3, 2n-4, 2n-1)\} \\ &\quad \{(2, 3, 4, ..., 2n-2, 2n-1, 2n)\} \\ \\ &= (1, 4i-8, 4i-12, 4i-16, ..., 12, 8, 4, 2n-1, 2n-5, \\ &\quad 2n, 5, 9, 13, ..., 4i-15, 4i-11, 4i-7) \\ &\quad (2, 2n-4, 2n-7, 2n-11, 2n-15, ..., 4i+9, 4i+5, \\ &\quad 4i+1, 4i-3, 4i-2, 4i+2, 4i+6, 4i+10, ..., 2n-10, \\ &\quad 2n-6, 2n-3, 2n-9, 2n-13, 2n-17, ..., 4i+3, \\ &\quad 4i-1, 4i-4, 4i, 4i+4, 4i+8, ..., 2n-12, 2n-8, 2n-2, \\ &\quad 3, 7, ..., 4i-9, 4i-5, 4i-6, 4i-10, ..., 14, 10, 6). \end{aligned}$$

El primero de los ciclos, involucra las cifras:

$$A := \{1, 5, 9, 13, ..., 4(i-2)+1, 2n-1, 2n-5\} \cup \{4, 8, 12, ..., , 4(i-2), 2n\}$$

y por tanto es un $2i$-ciclo. El segundo ciclo mueve las cifras restantes, por tanto será un $(2n-2i)$-ciclo. Basta aplicar el lema 2.1.3.

□

Aplicando los lemas 3.3.3, 3.3.4 y 3.3.7, el corolario 3.3.6 y el lema 2.1.1 hemos probado el siguiente teorema.

Teorema 3.3.8. *Sea σ una permutación en A_n que puede escribirse como producto de un número par de ciclos disjuntos de longitud par. Entonces σ es una palabra de Engel de longitud 2 en A_n.*

3.4. Resultado principal

En esta sección abordaremos el resultado central de éste capítulo.

Teorema 3.4.1. *Todo elemento de un grupo Alternado A_n, $n \geq 5$, puede escribirse como una palabra de Engel de longitud 2 en A_n.*

Recapitulemos, en primer lugar, los resultados probados en este capítulo. Podemos factorizar cualquier permutación $\sigma \in A_n$ como

$$\sigma = \tau_1 ... \tau_k \eta_1 ... \eta_r (\gamma_1 \gamma_2) ... (\gamma_{2s-1} \gamma_{2s}),$$

con τ_i 3-ciclos para todo i en $\{1, ..., k\}$, los η_j ciclos de longitud impar y mayor que 3 para todo j en $\{1, ..., r\}$ y los γ_t ciclos de longitud par para todo t en $\{1, ..., 2s\}$. (Puede que alguno de los tipos no aparezca).

Si no hay ciclos de longitud par involucrados en σ, es decir, $s = 0$, el teorema 3.2.5 asegura que σ es un elemento de $E_2(A_n)$. Del mismo modo, si no aparecen ciclos de longitud impar, es decir, $r = k = 0$, el teorema 3.3.8 asegura el resultado buscado.

En caso de que aparezca más de un ciclo de longitud impar en la factorización de σ, es decir, $k + r > 1$, el resultado se sigue del teorema 3.3.8 y el 3.2.5, pues nos permiten expresar $\tau_1 ... \tau_k \eta_1 ... \eta_r$ como una palabra de Engel de longitud 2 y $(\gamma_1 \gamma_2) ... (\gamma_{2s-1} \gamma_{2s})$ como otra palabra de Engel, siendo disjuntas las permutaciones que aparecen en ambas palabras de Engel, con lo que se puede usar el lema 2.1.1 para obtener el resultado.

El caso que permanece abierto es $k + r = 1$. Si $k = 0$ y $r = 1$ los lemas 3.1.3 y 3.1.4 nos aseguran que η_1 es una palabra de Engel de longitud 2 en $A_{sop(\eta_1)}$. Aplicando el teorema 3.2.5 sobre $\gamma = (\gamma_1 \gamma_2) ... (\gamma_{2s-1} \gamma_{2s})$ obtendremos otra palabra de Engel de longitud 2 en $A_{sop(\gamma)}$. Basta aplicar el lema 2.1.1 para resolver el problema en este caso.

Queda abordar el de permutaciones que se factorizan como un 3-ciclo por un producto de un número par de ciclos de longitud par (todos los ciclos disjuntos dos a dos), es decir, si $k = 1$ y $r = 0$.

Se abordará el problema siguiendo las mismas ideas usadas en la demostración del teorema 3.2.5.

Si $\lambda \in A_n$ es producto de dos ciclos disjuntos de longitud par, probaremos que λ se puede expresar como $E_2(\alpha, \beta)$, con $\alpha \in S_n$ y $\beta \in S_n \backslash A_n$.

De este modo, si $\sigma = (1, 2, 3)$ es un 3-ciclo podemos expresarlo como $E_2((1, 2, 3), (1, 2))$ si α es par ó como $E_2((1, 2), (1, 3))$ si α es impar. El lema 2.1.1 nos asegura que $\sigma\lambda \in E_2(A_n)$.

Comenzaremos estudiando el caso en el que ξ es una permutación de A_7 formada por un producto disjunto de un 3-ciclo y dos trasposiciones.

Lema 3.4.2. *Sea* $\xi = (1, 2, 3)(4, 5)(6, 7)$. *Se tiene que* ξ *es una palabra de Engel de longitud* 2 *en* A_7.

Demostración. Basta con observar que

$$\xi = E_2((1, 5, 2, 6, 3, 7, 4), (1, 5)(2, 6)(3, 4, 7)).$$

□

Comenzaremos estudiando los casos en que λ tiene soporte pequeño. En concreto, analizaremos lo que ocurre cuando λ mueve solamente seis cifras.

Lema 3.4.3. *Sea $\lambda = (3,5)(1,4,6,2)$ una permutación en A_6. Entonces existen $\alpha \in S_6$ y $\beta \in S_6 \backslash A_6$ tales que $\sigma = E_2(\alpha, \beta)$.*

Demostración. Basta observar que $\lambda = E_2((1,3,6),(1,2,3,4,5,6))$. □

Antes de abordar el caso general para una permutación λ que es un producto disjunto de un 2-ciclo y un ciclo de longitud par mayor o igual que 4 estudiaremos separadamente el caso $n = 8$, pues es algo distinto al caso general.

Lema 3.4.4. *Sea $\lambda = (1,5,6,7,2,8)(3,4)$ una permutación en A_8. Entonces existen $\alpha \in S_8$ y $\beta \in S_6 \backslash A_8$ tales que $\sigma = E_2(\alpha, \beta)$.*

Demostración. Basta observar que $\lambda = E_2((1,3)(2,8)(4,7),(1,2,3,4,5,6))$. □

Lema 3.4.5. *Sea $n \geq 8$ par. Consideremos una permutación σ en A_n que sea producto disjunto de un 2-ciclo y un $(n-2)$-ciclo. Entonces existen $\alpha \in S_n$ y $\beta \in S_n \backslash A_n$ tales que $\sigma = E_2(\alpha, \beta)$.*

Demostración. Consideremos las permutaciones siguientes:

$$\begin{aligned} \xi &= (1,3)(2,n)(4,n-1)(7,8)(9,10)...(n-3,n-2), \\ \tau &= (1,2,3,...,n-4,n-3,n-2). \end{aligned}$$

Se tiene

$$\begin{aligned} \gamma &= [\xi,\tau] = \xi^{-1}\gamma^{-1}\xi\gamma \\ &= \{(1,3)(2,n)(4,n-1)(7,8)(9,10)...(n-3,n-2)\} \\ &\quad \{(1,n-2,n-3,...,4,3,2)\} \\ &\quad \{(1,3)(2,n)(4,n-1)(7,8)(9,10)...(n-3,n-2)\} \\ &\quad \{(1,2,3,...,n-4,n-3,n-2)\} \\ &= (1,2,n-3,n-5,n-7,...,11,9,7,6,8,10,... \\ &\quad ...,n-8,n-6,n-4,n-2,n,3,4,n-1) \end{aligned}$$

Notemos que γ es un $(n-1)$-ciclo (pues el 5 queda fijo). Al conmutar γ y τ obtenemos:

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &= \{(1,n-1,4,3,n,n-2,n-4,n-6,...,10,8,6, \\ &\quad 7,9,11,13,...,n-9,n-7,n-5,n-3,2)\} \\ &\quad \{(1,n-2,n-3,...,4,3,2)\} \\ &\quad \{(1,2,n-3,n-5,n-7,...,11,9,7,6,8,10,... \\ &\quad ...,n-8,n-6,n-4,n-2,n,3,4,n-1)\} \\ &\quad \{(1,2,3,...,n-4,n-3,n-2)\} \end{aligned}$$

Consideremos dos casos:

- Si $n \equiv 0 \bmod(4)$ tenemos que

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &\quad (3,4)(1,n-6,n-10,n-14,...,10,6,5,9,13,... \\ &\quad ...,n-7,n-3,n-2,n-1,n-4,n-8,... \\ &\quad ...,12,8,7,11,15,...,n-9,n-5,2,n). \end{aligned}$$

- Si $n \equiv 2 \bmod(4)$ tenemos que

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &\quad (3,4)(1,n-6,n-10,n-14,...,12,8,7,11,15,... \\ &\quad ...,n-7,n-3,n-2,n-1,n-4,n-8,... \\ &\quad ...,10,6,5,9,13,...,n-9,n-5,2,n). \end{aligned}$$

En ambos casos $E_2(\xi,\tau)$ es producto de un 2-ciclo y un $(n-2)$-ciclo. Basta con aplicar ahora el lema 2.1.3. □

Antes de continuar con el estudio de productos de dos ciclos disjuntos de longitud par arbitraria, estudiaremos independientemente el caso en que $n = 8$ y queremos construir un producto de dos 4-ciclos como una palabra de Engel de longitud 2 en $E_2(A_8, S_8 \backslash A_8)$.

Lema 3.4.6. *Sea $n = 8$. Consideremos una permutación σ en A_8 que sea producto disjunto de un 4-ciclos. Entonces existen $\alpha \in S_8$ y $\beta \in S_8 \backslash A_8$ tales que $\sigma = E_2(\alpha,\beta)$.*

Demostración. Basta notar que

$$E_2((1,3)(2,8)(4,5)(6,7),(1,2,3,4,5,6)) = (1,2,7,8)(3,5,6,4)$$

y aplicar el lema 2.1.3 para obtener el resultado. □

Trataremos ahora el caso general.

Lema 3.4.7. *Sea $n \geq 10$ par y tomemos $2 \leq i \leq \lfloor n/4 \rfloor$. Consideremos una permutación σ en A_n que sea un producto disjunto de un $2i$-ciclo y un $(n-2i)$-ciclo. Entonces existen $\alpha \in S_n$ y $\beta \in S_n \backslash A_n$ tales que $\sigma = E_2(\alpha, \beta)$.*

Demostración. Consideremos las permutaciones siguientes:

$$\begin{aligned} \xi &= (1,3)(2,n)(4,5)(7,8)(9,10)...(2i+1,2i+2)(2i+3,n-1) \\ &\quad (2i+4,2i+5)(2i+6,2i+7)...(n-6,n-5)(n-4,n-3) \end{aligned}$$

$$\tau = (1,2,3,...,n-4,n-3,n-2).$$

Como en algunos resultados anteriores, para valores pequeños de n y de i la permutación ξ puede no quedar perfectamente clara. Conviene notar que para valores pequeños de n, los factores $(2i+3,n-1)(2i+4,2i+5)(2i+6,2i+7)...(n-6,n-5)(n-4,n-3)$ pueden desaparecer o verse reducidos a uno o dos. A continuación se dará explícitamente ξ en esos casos.

- Si $i \geq 5$, tenemos que $n \geq 20$ y la forma de ξ es clara.
- Si $i = 4$, se tiene que $n \geq 16$. Para $n = 16$ tendremos

$$\xi = (1,3)(2,16)(4,5)(7,8)(9,10)(11,15)(12,13).$$

- Si $i = 3$, se tiene que $n \geq 12$. Para $n = 12$ tendremos

$$\xi = (1,3)(2,12)(4,5)(7,11)(8,9).$$

- Si $i = 2$, se tiene que $n \geq 10$. Distinguiremos dos casos:
  - Si $n \geq 12$ la forma de ξ es clara. Si $n = 12$ se tiene que $2i+4 = n-4$ y $2i+5 = n-3$, es decir

$$\xi = (1,3)(2,12)(4,5)(7,11)(8,9)$$

  - Si $n = 10$, la permutación ξ será

$$\xi = (1,3)(2,10)(4,5)(7,9) = (1,3)(2,n)(4,5)(2i+3,n-1).$$

Tratemos ahora el caso general, tendremos que

$$\begin{aligned}
\gamma &= [\xi,\tau] = \xi^{-1}\tau^{-1}\xi\tau \\
&= \{(1,3)(2,n)(4,5)(7,8)(9,10)...(2i+1,2i+2)(2i+3,n-1) \\
&\quad (2i+4,2i+5)(2i+6,2i+7)...(n-6,n-5)(n-4,n-3)\} \\
&\quad \{(1,n-2,n-3,...,4,3,2)\} \\
&\quad \{(1,3)(2,n)(4,5)(7,8)(9,10)...(2i+1,2i+2)(2i+3,n-1)\} \\
&\quad \{(2i+4,2i+5)(2i+6,2i+7)...(n-6,n-5)(n-4,n-3)\} \\
&\quad \{(1,2,3,...,n-4,n-3,n-2)\} \\
&= (1,2,n-2,n,3,5,4) \\
&\quad (6,8,10,...,2i,2i+2,2i+3,2i+5,...,n-7,n-5,n-3, \\
&\quad n-4,n-6,...,2i+6,2i+4,n-1,2i+1,2i-1,...,11,9,7).
\end{aligned}$$

Notemos que el $sop(\gamma) = \{1,2,...,n\}$. Al conmutar γ y τ de nuevo obtenemos

$$\begin{aligned}
E_2(\xi,\tau) &= [\gamma,\tau] \\
&= \{(1,4,5,3,n,n-2,2) \\
&\quad (6,7,9,11,...,2i-3,2i-1,2i+1,n-1,2i+4, \\
&\quad 2i+6,...,n-6,n-4,n-3,n-5,n-7,...,2i+5, \\
&\quad 2i+3,2i+2,2i,2i-2,...,12,10,8)\} \\
&\quad \{(1,n-2,n-3,...,4,3,2)\} \\
&\quad \{(1,2,n-2,n,3,5,4) \\
&\quad (6,8,10,...,2i,2i+2,2i+3,2i+5,...,n-7,n-5,n-3, \\
&\quad n-4,n-6,...,2i+6,2i+4,n-1,2i+1,2i-1,...,11,9,7)\} \\
&\quad \{(1,2,3,...,n-4,n-3,n-2)\}.
\end{aligned}$$

Consideraremos 4 casos:

- Si $n, 2i \equiv 0 \bmod(4)$ tendremos que

$$\begin{aligned}
E_2(\xi,\tau) &= [\gamma,\tau] \\
&\quad (1,n-5,n-9,...,2i+7,2i+3,2i+4,2i+8,..., \\
&\quad ...,n-12,n-8,n-4,n-7,n-11,...,2i+9,2i+5, \\
&\quad 2i+2,2i+6,...,n-10,n-6,n-3,n-2,4,n) \\
&\quad (2,5,9,...,2i-7,2i-3,2i-1,2i,2i-4,2i-8,..., \\
&\quad ...,12,8,7,11,...,2i-5,2i-1,n-1,2i-2,2i-6,...,10,6,3).
\end{aligned}$$

- Si $n \equiv 2 \bmod(4)$ y $2i \equiv 0 \bmod(4)$ tendremos que

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &(1, n-5, n-9, ..., 2i+9, 2i+5, 2i+2, 2i+6, ..., \\ &..., n-12, n-8, n-4, n-7, n-11, ..., 2i+3, 2i+4, \\ &2i+8, ..., n-10, n-6, n-3, n-2, 4, n) \\ &(2, 5, 9, ..., 2i-7, 2i-3, 2i-1, 2i, 2i-4, 2i-8, ..., \\ &..., 12, 8, 7, 11, ..., 2i-5, 2i-1, n-1, 2i-2, 2i-6, ... \\ &..., 10, 6, 3). \end{aligned}$$

- Si $n \equiv 0 \bmod(4)$ y $2i \equiv 2 \bmod(4)$ tendremos que

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &(1, n-5, n-9, ..., 2i+9, 2i+5, 2i+2, 2i+6, ..., \\ &..., n-12, n-8, n-4, n-7, n-11, ..., 2i+3, 2i+4, \\ &2i+8, ..., n-10, n-6, n-3, n-2, 4, n) \\ &(2, 5, 9, ..., 2i-9, 2i-5, 2i-1, n-1, 2i-2, 2i-6, ... \\ &..., 12, 8, 7, 11, ..., 2i-7, 2i-3, 2i+1, 2i, 2i-4, \\ &2i-8, ..., 10, 6, 3). \end{aligned}$$

- Si $n, 2i \equiv 2 \bmod(4)$ tendremos que

$$\begin{aligned} E_2(\xi,\tau) &= [\gamma,\tau] \\ &(1, n-5, n-9, ..., 2i+7, 2i+3, 2i+4, 2i+8, ..., \\ &..., n-12, n-8, n-4, n-7, n-11, ..., 2i+9, 2i+5, \\ &2i+2, 2i+6, ..., n-10, n-6, n-3, n-2, 4, n) \\ &(2, 5, 9, ..., 2i-9, 2i-5, 2i-1, n-1, 2i-2, 2i-6, ... \\ &..., 12, 8, 7, 11, ..., 2i-7, 2i-3, 2i+1, 2i, 2i-4, \\ &2i-8, ..., 10, 6, 3). \end{aligned}$$

En todos los casos $E_2(\xi,\tau)$ es un producto de un $2i$-ciclo y un $(n-2i)$-ciclo. De nuevo, basta aplicar el lema 2.1.3 para asegurar el resultado.

□

Con todo lo realizado hasta el momento, hemos demostrado el siguiente resultado.

Corolario 3.4.8. *Sea σ una permutación en A_n que es un producto de dos ciclos disjuntos de longitud par τ_1 y τ_2, con $\sharp sop(\tau_1) \geq 4$. Entonces existen $\alpha \in S_{sop(\sigma)}$ y $\beta \in S_{sop(\sigma)} \backslash A_{sop(\sigma)}$ tales que $\sigma = E_2(\alpha,\beta)$.*

El siguiente corolario recoge toda la información obtenida en los anteriores resultados.

Corolario 3.4.9. *Sea $n \geq 7$. Toda permutación σ en A_n formada por un producto disjunto de un 3-ciclo y de dos ciclos de longitud par es una palabra de Engel de longitud 2 en A_n.*

Demostración. Si $n = 7$ u 8, el lema 3.4.2 resuelve el problema.

Supongamos entonces que $n > 8$ y sean τ_1 y τ_2 ciclos de longitud par, con $\sharp sop(\tau_1) \geq 4$. Gracias al corolario 3.4.8 se tiene que existe $\alpha \in S_{sop(\tau_1\tau_2)}$ y $\beta \in S_{sop(\tau_1\tau_2)} \backslash A_{sop(\tau_1\tau_2)}$ tales que $\tau_1\tau_2 = E_2(\alpha, \beta)$.

Basta con observar que un 3-ciclo, por ejemplo, el $(1, 2, 3)$ puede expresarse de dos maneras diferentes:

$$(1, 2, 3) = E_2((1, 2, 3), (2, 3)) = E_2((1, 2), (1, 3)).$$

De este modo, si $\sigma = (1, 2, 3)\tau_1\tau_2$, con τ_i ciclos de longitud par para $i = 1, 2$, podemos aplicar el lema 2.1.1 a lo anterior para obtener que

- Si α es una permutación en A_n, tenemos que

$$\sigma = E_2((1, 2, 3), (2, 3))E_2(\alpha, \beta) = E_2((1, 2, 3)\alpha, (2, 3)\beta) \in E_2(A_n).$$

- Si α es una permutación en $S_n \backslash A_n$, tenemos que

$$\sigma = E_2((1, 2), (1, 3))E_2(\alpha, \beta) = E_2((1, 2)\alpha, (1, 3)\beta) \in E_2(A_n).$$

□

Por tanto, acabamos de probar ya el resultado central de este capítulo, el teorema 3.4.1.

Capítulo 4

Aproximación combinatoria y computacional

Una vez probado que todo elemento del grupo alternado A_n se puede escribir como una palabra de Engel de longitud 2 en A_n, se intentará ver que ocurre al trabajar con palabras de Engel de longitudes superiores.

Mucha de la información obtenida en capítulos anteriores acerca de qué elementos pueden ser escritos como palabras de Engel de longitud dos se puede extender a palabras de Engel de longitud arbitraria. Pero los resultados en los que se da una construcción explicita de la palabra de Engel de longitud 2 a partir de permutaciones adecuadas no son extensibles a longitudes mayores, por lo que es necesario buscar otros métodos.

En primer lugar trataremos de buscar un método que nos permita comprobar la tesis para grupos alternados de grados pequeños.

Para el desarrollo de este capítulo se ha hecho uso del lenguaje de programación GAP para realizar los cálculos sobre el grupo alternado A_n. Hay que hacer notar que GAP realiza la multiplicación dentro del grupo Simétrico en orden contrario al que se ha utilizado en capítulos anteriores, lo que debe tenerse en cuenta.

4.1. Grafos de Engel

En esta sección construiremos un grafo, asociado a un grupo alternado A_n y una permutación y en A_n, que nos facilitará el estudio empírico de las palabras de Engel de la forma $E_m(\cdot, y)$ en A_n.

Fijado un elemento y en un grupo alternado A_n, con $n \geq 5$, y un $m \geq 1$, consideremos el conjunto de palabras de Engel de longitud m:

$$E_m(y) := \{E_m(x, y) \mid x \in A_n\}.$$

Puesto que para todo $m \geq 1$ tenemos que $E_{m+1}(y) \subset E_m(y)$ tenemos que $\{E_m(y)\}_{m\geq 0}$ es un cadena descendente de subconjuntos de A_n.

Fijado $m \geq 1$, podemos ver $E_m(y)$ como $\{[x, y] \mid x \in E_{m-1}(y)\}$. De este modo si $x, z \in E_{m-1}(y)$ tendremos que

$$[x, y] = [z, y] \quad \text{si y sólo si} \quad C_{A_n}(y)x = C_{A_n}(y)z.$$

Así, si denotamos por $\Omega_m^y := \{C_{A_n}(y)x \mid x \in E_{m-1}(y)\}$, podemos construir la aplicación

$$\begin{array}{rccc} \varphi_m : & \Omega_m^y & \longrightarrow & E_m(y) \\ & C_{A_n}(y)x & \mapsto & [x, y] \end{array} \tag{4.1}$$

Lema 4.1.1. *Para todo $m \geq 1$ y para todo elemento $y \in A_n$, $n \geq 5$, la aplicación φ_m está bien definida y es biyectiva.*

De esta manera, se pueden estudiar los conjuntos $E_m(y)$ trabajando con las clases a derecha módulo $C_{A_n}(y)$.

Es evidente que $\{\Omega_m^y\}_{m\geq 1}$ es una cadena descendente de conjuntos. Además, como A_n es un grupo finito, tendremos que siempre existirá un $m \in \mathbb{N}$ para el que $\Omega_m^y = \Omega_{m+1}^y$, por lo que la cadena siempre se estabiliza a partir de cierto número natural.

Podemos construir un grafo dirigido en el que se pueda estudiar la dinámica de las palabras de Engel sobre A_n.

Consideremos el conjunto de vértices $V_n^y := \Omega_1^y$. El conjunto $\mathbb{A}$ de aristas del grafo, se define con la siguiente relación:

- Dados $z_1, z_2 \in V_n^y$, existe una arista que parte de z_1 y llega a z_2 si y sólo si $C_{A_n}(y)[z_1, y] = C_{A_n}(y)z_2$.

Definición 4.1.1. *Fijado un elemento y del grupo alternado A_n, el grafo $(V_n^y, \mathbb{A})$ se denomina grafo de Engel asociado al elemento y en el grupo alternado A_n.*

Indiquemos ahora algunas consecuencias de la introducción del grafo de Engel.

- Si consideramos un camino de longitud k en el grafo, que parte del vértice $C_{A_n}(y)z_1$ y termina en el vértice $C_{A_n}(y)z_{k+1}$, tendremos que $E_k(z_1, y) = [z_{k+1}, y]$. De este modo, calcular palabras de Engel de longitud elevada es mucho más sencillo.

- Recíprocamente, si queremos conocer $E_k(x,y)$, basta considerar un camino de longitud k que comienza en el vértice $C_{A_n}(y)x$ y conmutar con y un representante de la clase módulo $C_{A_n}(y)$ asociada al vértice anterior al último vértice del camino, $C_{A_n}(y)z_{k_1}$. De este modo, tendremos que
$$E_k(x,y) = [z_{k-1}, y].$$
- Estudiar la dinámica del conjunto $\{E_m(\cdot,y)\}_{m\geq 0}$ se reduce a estudiar la dinámica del grafo $(V_n^y, \mathbb{A})$.

Una vez hemos construído el grafo, parece natural plantearnos pensar cuándo podremos afirmar mediante el estudio del grafo Engel que un elemento del grupo alternado A_n, $n \geq 5$, es una palabra de Engel de la forma $E_m(\cdot,y)$ para todo $m \geq 1$. O alternativamente, si es posible saber a partir del grafo de Engel cuando un elemento no será una palabra de Engel de longitud arbitraria de la forma $E_m(\cdot,y)$.

Para ello, estudiaremos los ciclos dirigidos de un grafo de Engel $(V_n^y, \mathbb{A})$.

Lema 4.1.2. *Sea φ_1 la aplicación 4.1 con $m = 1$. Si (W,β) es un ciclo dirigido de $(V_n^y, \mathbb{A})$, todos los elementos del conjunto $\varphi_1(W)$ se pueden escribir como palabras de Engel de longitud arbitraria.*

Demostración. Consideremos (W,β) un ciclo dirigido del grafo de Engel $(V_n^y, \mathbb{A})$.

Fijado un elemento inicial arbitrario $C_{A_n}(y)x$ dentro de W, tenemos que
$$\varphi_1(W) := \{E_k(x,y) \mid k \in \mathbb{N}\}.$$

Pero debido a que W es un ciclo dirigido, existe $k_1 \in \mathbb{N}$ verificando que $[x,y] = E_{k_1}(x,y)$.

Elijamos un entero $m \in \mathbb{N}$ y tomemos una permutación σ del conjunto $\varphi_1(W)$. Se tiene que existe $z \in C_{A_n}(y)x$ tal que $\sigma = [z,y]$ y que existe $k_2 \in \mathbb{N}$ verificando que $[z,y] = E_{k_2}(z,y) = E_{2k_2}(z,y) = ... = E_{rk_2}(z,y)$, con $r \in \mathbb{N}$.

Basta tomar $k_2 > m$ para obtener que $\sigma = E_m(\tau,y)$ para algún $\tau \in A_n$. □

Así pues, fijado un grupo alternado A_n, $n \geq 5$, y un elemento y en dicho grupo, basta estudiar los ciclos dirigidos en el grafo de Engel asociado para obtener un subconjunto de elementos de A_n que puede ser escrito como palabras de Engel de longitud arbitraria.

De hecho, sabremos que si $z \in \varphi_1(W)$, siendo W un ciclo dirigido en un grafo de Engel, $z = E_m(v(m),y)$ para todo $m \in \mathbb{N}$, con $v(m) \in A_n$ (y dependiente de m).

Corolario 4.1.3. *Si (W, β) es un ciclo dirigido de $(V_n^y, \mathbb{A})$ y φ_1 la aplicación 4.1 con $m = 1$, todo elemento de $\varphi_1(W)^{S_n}$ se puede escribir como una palabra de Engel de longitud arbitraria en A_n.*

Demostración. La demostración es consecuencia directa de los lemas 2.1.3 y 4.1.2. □

4.2. Grupos alternados pequeños

En esta sección utilizaremos el grafo de Engel definido anteriormente para probar que $A_n = E_m(A_n)$ para todo $m \geq 1$ y para todo $n \leq 14$. Comenzaremos trabajando con el grupo alternado A_5.

Aun siendo el caso más sencillo, el pequeño soporte de A_5 hace que el grupo se comporte de manera algo distinta a los grupos alternados de orden mayor. En primer lugar, fijaremos un elemento y para calcular el grafo de Engel $(V_5^y, \mathbb{A})$.

Consideremos $y := (1, 2, 3, 4, 5)$ un 5-ciclo en A_5. Se tiene que $C_{A_5}(y) = \langle y \rangle$, que es un grupo cíclico de orden 5, por lo que $V_5^y = \{\langle y \rangle x \mid x \in A_5\}$ es un conjunto de cardinal $\mid A_5 : \langle y \rangle \mid = 12$.

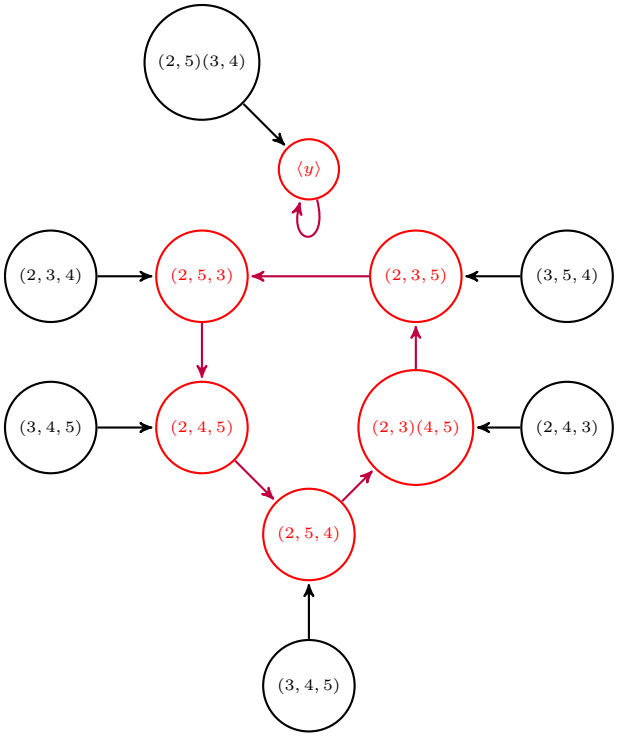
Construiremos el grafo de Engel $(V_5^y, \mathbb{A})$. Como ya sabemos, cada vértice del grafo está asociado a una clase a derecha módulo $C_{A_5}(y)$. Para simplificar la notación, denotaremos a cada vértice por una permutación de la clase a la que representa. Es decir, si el vértice está representado por una permutación σ, dicho vértice, representa en realidad la clase $\langle y \rangle \sigma$ de V_5^y.

A la vista del grafo, que se muestra en la siguiente página, se ve que hay dos ciclos dirigidos. El primero de ellos, W_1, es el ciclo de los cinco elementos centrales del grafo y el otro, W_2, el que forma la clase del neutro por sí misma.

Haciendo uso del lema 4.1.2, tendremos que calcular los conjuntos $\varphi_1(W_1)$ y $\varphi_1(W_2)$ para conocer un conjunto de elementos de A_5 que pueden ser escrito como palabras de Engel de orden arbitrario. De éste modo, tendremos que:

$$\varphi_1(W_2) := \{e\},$$

$$\varphi_1(W_1) := \{(1, 3, 2, 5, 4), (1, 3, 5, 4, 2), (1, 4, 3, 5, 2), (1, 5, 2, 4, 3), (1, 5, 3, 2, 4)\}.$$



Así, gracias al corolario 4.1.3 tendremos que todo 5-ciclo de A_5 es una palabra de Engel de longitud arbitraria en A_5. Teniendo en cuenta este hecho junto con los lemas 2.2.3, 2.2.4 y 2.1.3 podemos enunciar el siguiente resultado:

Teorema 4.2.1. *Todo elemento de A_5 puede ser escrito como una palabra de Engel de longitud arbitraria. Es decir, para todo $n \geq 1$ se tiene que $A_5 = E_n(A_5)$.*

Aunque este resultado ya se podría haber dado con el trabajo hecho en las secciones anteriores, para grupos alternados de orden mayor (incluso A_6), ya no podemos deducir el resultado análogo y el trabajo con el grafo de Engel nos permitirá probar el análogo de 4.2.1 para otros grupos alternados de grado mayor.

Antes de comenzar con grupos alternados de grado mayor, conviene observar cómo se comportan los ciclos dirigidos de un grafo de Engel al aumentar el orden de grupo alternado con el que se trabaja.

Lema 4.2.2. *Si $m \geq n$ y $\phi : A_n \longrightarrow A_m$ es la incrustación natural, la imagen por ϕ de un ciclo dirigido del grafo de Engel $(V_n^y, \mathbb{A})$, será un ciclo dirigido del grafo de Engel $(V_m^y, \mathbb{B})$.*

Demostración. Fijado $y \in A_n$ y considerando un ciclo dirigido W_1 del grafo de Engel $(V_n^y, \mathbb{A})$. Dado un vértice $C_{A_n}(y)x$ de W_1, podemos considerar el ciclo dirigido W_2 de $(V_m^y, \mathbb{B})$, que contiene como elemento a $C_{A_m}(y)x$.

Si hay una arista entre dos vértices x, z de W_1, tendremos que

$$C_{A_n}(y)[x, y] = C_{A_n}(y)z.$$

Esto implica que $[x, y]z^{-1} \in C_{A_n}(y) \subset C_{A_m}(y)$ para todo $m \geq n$. De este modo, si hay una arista entre dos vértices x, z de W_1, habrá una arista entre la imagen de esos mismos vértices por la aplicación ϕ en el ciclo dirigido W_2. Como W_1 es un ciclo dirigido, se tiene que W_2 es otro ciclo dirigido de la misma longitud que W_1.

□

Además, este lema nos permite enunciar un corolario que ya se había demostrado en las secciones anteriores.

Corolario 4.2.3. *Todo elemento de A_n que es una palabra de Engel de longitud arbitraria en A_n, es también una palabra de Engel de longitud arbitraria en A_m, para todo $m \geq n$.*

Se verá ahora una condición suficiente para que dos grafos de Engel sean isomorfos.

Lema 4.2.4. *Si $z \in Cl_{S_n}(y)$ entonces se tiene que los grafos de Engel $(V_n^y, \mathbb{A})$ y $(V_n^z, \mathbb{B})$ son isomorfos.*

Demostración. Escribamos $z := y^x$ para algún $x \in S_n$. Basta definir el isomorfismo de grafos como sigue:

$$\begin{aligned} \phi : V_n^y &\longrightarrow V_n^z \\ C_{A_n}(y)\sigma &\mapsto C_{A_n}(z)\sigma^x \end{aligned}$$

Si $C_{A_n}(y)x_1 = C_{A_n}(y)x_2$, se tiene que $x_1x_2^{-1} \in C_{A_n}(y)$. Así, se tiene que

$$(x_2x_1^{-1})^x y^x (x_1x_2^{-1})^x = y^x,$$

de dónde se sigue que $C_{A_n}(z)x_1^x = C_{A_n}(z)x_2^x$ y por tanto, ϕ es inyectiva.

La suprayectividad es evidente, por lo que ϕ es una biyección.

Consideremos ahora dos vértices $C_{A_n}(y)x_1$ y $C_{A_n}(y)x_2$ en $(V_n^y, \mathbb{A})$, de manera que existe una arista de $C_{A_n}(y)x_1$ a $C_{A_n}(y)x_2$, esto es $C_{A_n}(y)[x_1.y] = C_{A_n}(y)x_2$.

Así, tendremos que

$$x_2[x_1, y]^{-1} y[x_1, y] x_2^{-1} = y,$$

de dónde se obtiene que

$$(x_2[x_1, y]^{-1})^x y^x ([x_1, y] x_2^{-1})^x = y^x,$$

para concluir que

$$C_{A_n}(z)[x_1^x, z] = C_{A_n}(z) x_2^x.$$

De este modo hemos probado que si existe una arista entre dos vértices de $(V_n^y, \mathbb{A})$, también la habrá entre las imágenes de esos dos vértices por ϕ. La demostración de la relación inversa es análoga, obteniendo finalmente que ϕ es un isomorfismo de grafos. □

Se podría pensar en usar la matriz de adyacencia del grafo de Engel para estudiar qué vértices pertenecen a un ciclo dirigido. Si consideramos Λ la matriz de adyacencia asociada al grafo de Engel $(V_n^y, \mathbb{A})$, se tiene el elemento a_{ij} de la matriz Λ^k nos indica el número de caminos de longitud k que van del vértice i al vértice j del grafo.

Así, haciendo sucesivas potencias de la matriz y observando cuando los elementos de la diagonal de Λ^k van resultando distintos de 0, podremos calcular los elementos que pertenecen a ciclos dirigidos del grafo de Engel.

Si consideramos el grafo $(V_5^y, \mathbb{A})$, con $y := (1, 2, 3, 4, 5)$, tendremos que una matriz de adyacencia Λ asociada al grafo es:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}$$

Si ahora calculamos Λ^5, el resultado es:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Dónde se puede observar que hay 6 nodos del grafo de Engel $(V_5^y, \mathbb{A})$ en ciclos dirigidos. Si nos fijamos en el grafo construido en 4.2, nos damos cuenta que de hecho, esos son los 6 nodos que forman los ciclos dirigidos del grafo.

Pero trabajar con estas matrices se vuelve inviable en cuanto se aumenta el orden del grupo alternado, pues el número de nodos del grafo aumenta mucho. Por ejemplo, ya en A_6 para $y = (1, 2, 3, 4, 5)$ el conjunto V_6^y tiene $\mid A_6 \mid / \mid C_{A_6}(y) \mid = 72$ elementos. Además, es necesario calcular las distintas potencias de la matriz para encontrar los ciclos dirigidos del grafo, y en principio, no sabríamos cuantas potencias son necesarias.

Un posible test de parada podría ser encontrar dos números enteros k_1, k_2 para los cuales $A^{k_1} = A^{k_2}$. En ese caso, las matrices del conjunto $M_\Lambda := \{\Lambda^k \mid k_1 \leq k \leq k_2 - 1\}$ contendrían la información sobre los ciclos dirigidos del grafo de Engel asociado a la matriz de adyacencia Λ.

Si consideramos el ejemplo anterior, tendríamos que A^{10} es igual que A^5, por lo que sólo habría que estudiar 4 matrices para calcular y conocer los elementos que pertenecen a los ciclos dirigidos del grafo.

El problema que este método presenta es que el tanto el tamaño del conjunto M_Λ como el de la matriz de adyacencia A pueden ser muy grandes y habría que estudiar un número elevado matrices de gran tamaño. Conviene por tanto buscar otra manera de estudiar estos grafos sin hacer uso de la matriz de adyacencia.

Para trabajar con grupos de órdenes mayores hemos usado el lenguaje de programación GAP. Se ha programado un script que calcula los ciclos dirigidos $\{W_k\}$ del grafo de Engel asociado a un grupo alternado A_n y a un elemento $y \in A_n$.

Posteriormente calcula el conjunto $\varphi_1(W_k)$ para cada ciclo dirigido W_k y nos da como output los tipos de permutaciones de A_n que no aparecen en

$\cup_k \varphi_1(W_k)$.

Estos tipos de permutaciones serán elementos de A_n que no pueden ser escritos como palabras de Engel de longitud arbitraria de la forma $E_m(x,y)^\sigma = E_m(x^\sigma, y^\sigma)$.

El pseudocódigo del algoritmo utilizado para los grupos más pequeños es el siguiente:

```
1: G:=AlternatingGroup(n); # Siendo n el entero que deseemos.
2: G1:=SymmetricGroup(n);
3: H:=G;
4: i:=0;
5: Sld:=Size(G);
6: y:= ... ; # Siendo y la permutación a estudio.
7: while Sld>0 do
8:     A:=[];
9:     A:=Set(A);
10:    i=i+1;
11:    for x in G  do
12:        x:=Comm(x,y);
13:        AddSet(A,x);
14:    end for
15:    Sld:=Size(G)-Size(A);
16:    G:=A;
17: end while
18: k:=Size(A);
19: U:=Centralizer(H,y);
20: B:=[];
21: B:=Set(B);
22: t:=0;
23: P:=A;
24: M:=[];
25: M:=Set(M);
26: F:=[];
27: while Size(A)>0 do
28:    for x in A do
29:        t:=t+1;
30:        while x in A do
31:            AddSet(M,x);
32:            RemoveSet(A,x);
33:            z:=CanonicalRightCosetElement(U,x);
```

```
34:             AddSet(B,z);
35:             x:=Comm(z,y);
36:         end while
37:         f:=Size(B);
38:         Print(El ciclo dirigido t y sus f conmutadores asociados:);
39:         Print(B, mod C_{A_n}(y) );
40:         Print(M);
41:         Clases:=Set([]);
42:         for x in M do
43:             AddSet(Clases,x^{G_1});
44:         end for
45:     end for
46: end while
47: AddSet(F,f);
48: B:=[];
49: M:=[];
50: B:=Set(B);
51: M:=Set(M);
52: M1:=Set(ConjugacyClasses(G_1));
53: M2:=Set([]);
54: for u in M1 do
55:     u1:=Representative(u);
56:     if u1 in G then
57:         AddSet( M2, u );
58:     end if
59: end for
60: if Size(Clases)=Size(M2) then
61:     Print(Hay al menos un elemento de cada clase de conjugación de A_n
        en los ciclos dirigidos.);
62: else
63:     SubtractSet( M2, Clases );
64:     Print(Los elementos de las clases de conjugación: M2 no son palabras
        de Engel de longitud arbitraria de tipo E_m(·, y));
65: end if
```

Fijamos un ciclo y de longitud máxima en A_n, $5 \leq n \leq 14$, y haremos uso del algoritmo anterior para construir los ciclos dirigidos del grafo de Engel $(V_n^y, \mathbb{A})$ y observaremos si se cumple el teorema 4.2.1 para otros grupos alternados pequeños.

La idea es calcular el conjunto $\Omega := \cup_k \varphi_1(W_k)$, dónde W_k recorre los

ciclos del grafo de Engel en el que estemos trabajando, y buscar los tipos de permutaciones de A_n que no aparecen en dicho conjunto.

- Al aplicar el algoritmo anterior en A_6 para $y = (1, 2, 3, 4, 5)$ obtenemos que los tipos de permutaciones de A_6 que no aparecen en el conjunto Ω son
$$\{(1, 2)(3, 4), (1, 2, 3), (1, 2, 3)(4, 5, 6)\}.$$
Basta entonces observar los resultados 2.2.3, 2.2.4 y 2.1.8, ya obtenidos en secciones anteriores para obtener el análogo de 4.2.1 para el grupo A_6.

- Para los grupos alternados A_n, con $7 \leq n \leq 14$, ocurre algo parecido. Al aplicar el algoritmo anterior para $y = (1, 2, 3, ..., n)$, si n es impar, o $y = (1, 2, 3, ..., n-1)$ si n es par y observar el conjunto Ω, el único tipo de permutación de A_n que no pertenece al conjunto Ω es $\{(1, 2)(3, 4)\}$.
De este modo, basta con aplicar el lema 2.2.3 para obtener el resultado deseado.

La siguiente tabla recopila el resumen de la información obtenida computacionalmente.

Grupo	C. de Conj. no encontradas	Tiempo de Ejecución
A_5	$\{(1, 2)(3, 4)^{S_5}, (1, 2, 3)^{S_5}\}$	7 mmsec
A_6	$\{(1, 2)(3, 4)^{S_6}, (1, 2, 3)^{S_6}$, $(1, 2, 3)(4, 5, 6)^{S_6}\}$	18 mmsec
A_7	$\{(1, 2)(3, 4)^{S_7}\}$	40 mmsec
A_8	$\{(1, 2)(3, 4)^{S_8}\}$	201 mmsec
A_9	$\{(1, 2)(3, 4)^{S_9}\}$	4 seg 12 mmsec
A_{10}	$\{(1, 2)(3, 4)^{S_{10}}\}$	40 seg 809 mmsec
A_{11}	$\{(1, 2)(3, 4)^{S_{11}}\}$	5 min 37 seg 139 mmsec
A_{12}	$\{(1, 2)(3, 4)^{S_{12}}\}$	63 min 38 seg 210 mmsec
A_{13}	$\{(1, 2)(3, 4)^{S_{13}}\}$	21 h 6 min 54 seg
A_{14}	$\{(1, 2)(3, 4)^{S_{14}}\}$	$>$ 12 días

Cuadro 4.1: Clases de conjugación de elementos de A_n en S_n no encontradas en los ciclos dirigidos del grafo.

Es decir, los cálculos computacionales juntos con algunos resultados de capítulos anteriores nos permiten enunciar el siguiente teorema.

Teorema 4.2.5. *Fijado $5 \leq n \leq 14$, todo elemento del grupo alternado A_n puede ser escrito como una palabra de Engel de longitud arbitraria en A_n, es decir,*

$$A_n = E_m(A_n).$$

4.3. Cadenas de Engel

En la sección anterior hemos fijado un elemento y de un grupo alternado A_n y hemos considerado las clases $\{C_{A_n}(y)x \mid x \in A_n\}$. Trabajando con dichas clases hemos construído los grafos de Engel que nos han permitido probar el teorema 4.2.5.

En esta sección trabajaremos con las palabras de Engel, obteniendo información adicional sobre su comportamiento en el grupo alternado.

Fijado un elemento y en el grupo alternado A_n, $n \geq 5$, para cada elemento $x \in A_n$ podemos considerar la serie de palabras de Engel

$$E^y(x) := \{x, E_1(x,y), E_2(x,y), ...\}.$$

Es evidente que llegará un momento en que los elementos de $E^y(x)$ comiencen a repetirse. Es decir, siempre existirán dos enteros $1 \leq k_1 < k_2$ tales que $E_{k_1}(x,y) = E_{k_2}(x,y)$ en $E^y(x)$. Consideremos

$$B^y(x) := \{E_{k_1}(x,y), ..., E_{k_2-1}(x,y)\}.$$

Definición 4.3.1. *Fijados elementos x, y en A_n. El conjunto $E^y(x)$ se llama cadena asociada al elemento x y $B^y(x)$ bucle asociado al elemento x.*

La longitud de la cadena $E^y(x)$ será $l(E^y(x)) = k_2 - 1$ y la longitud del bucle será $l(B^y(x)) = k_2 - k_1$.

Lema 4.3.1. *Fijado $n \geq 5$ se tiene que, para todo $m \in \mathbb{N}$*

$$E_m(x,y)E_{m+1}(x,y) = E_m(x^y, y).$$

Demostración. Fijado $y \in A_n$, se tiene que para todo $m \in \mathbb{N}$

$$E_m(x,y)^y = E_m(x^y, y).$$

Así, tendremos que

$$E_m(x^y, y) = E_m(x,y)(E_m(x,y))^{-1}y^{-1}E_m(x,y)y = E_m(x,y)E_{m+1}(x,y).$$

□

Es decir, el resultado anterior nos garantiza que el producto de dos palabras de Engel consecutivas en una cadena $E^y(x)$ es una palabra de Engel de la cadena $E^y(x^y)$.

Definición 4.3.2. *Fijados dos elementos x e $y \in A_n$, con $n \geq 5$. El bucle $B^y(x)$ se dirá estable por y-conjugación si $(B^y(x))^y = B^y(x)$.*

Podemos dar una caracterización de la estabilidad por y-conjugación gracias al lema 4.3.1.

Lema 4.3.2. *Fijados dos elementos x e $y \in A_n$, con $n \geq 5$, el bucle $B^y(x)$ es estable por y-conjugación si y sólo si para todo $E_m(x,y) \in B^y(x)$ se verifica que*

$$E_m(x,y)E_{m+1}(x,y) \in B^y(x).$$

Demostración. Basta observar que

$$(B^y(x))^y := \{E_m(x,y)^y \mid E_m(x,y) \in B^y(x)\},$$

y que $E_m(x,y)^y = E_m(x^y,y)$.

Basta hacer uso del lema 4.3.1 para completar la demostración. □

En el siguiente lema, se enuncia otra propiedad importante sobre bucles estables por y-conjugación para un tipo de permutación en un grupo alternado A_n.

Lema 4.3.3. *Sea $y \in A_n$ un ciclo de longitud máxima y $B^y(x)$ un bucle estable por y-conjugación. Tomemos $\delta \in B^y(x)$. Se verifica que*

1. *Para todo $z \in C_{A_n}(y)\delta$ se tiene que $[\delta, y] = [z, y]$.*

2. *Para todo $z \in \delta C_{A_n}(y)$ se tiene que $[z, y] \in B^y(x)$.*

Demostración. El punto (1) es evidente. Para probar el punto (2), como $C_{A_n}(y) = \langle y \rangle$ se tiene que

$$[\delta, y]^y = y^{-1}\delta^{-1}y^{-1}\delta yy = [\delta y, y],$$

y por tanto, lo mismo ocurre con todas las potencias de y, de donde se obtiene el resultado.

□

Gracias al lema anterior sabemos que si tomamos un elemento δ de un bucle $B^y(x)$ estable por y-conjugación, todo elemento del conjunto $C_{A_n}(y)\delta$ da el mismo resultado al ser conmutado por y. Además, δ será el único elemento del conjunto $C_{A_n}(y)\delta$ que pertenece a $B^y(x)$.

Por otro lado, todo elemento del conjunto $\delta C_{A_n}(y)$ pertenecerá al bucle $B^y(x)$ al ser conmutado por y y además, teniendo en cuenta que y es un ciclo de longitud máxima en A_n, tendremos que

$$\delta C_{A_n}(y) = \{[\delta, y]^{y^j} \mid j = 1, ..., o(\delta)\}.$$

Se tiene también que la condición (2) del lema anterior es necesaria y suficiente para garantizar la estabilidad por y-conjugación del bucle $B^y(x)$.

Para continuar, se va a dar una propiedad relacionada con lo anterior para el caso de grupos alternados A_p, con p un número primo.

Lema 4.3.4. *Consideremos p un número primo e $y \in A_p$ un p-ciclo. Si el bucle $\beta^y(x)$ no es estable por y-conjugación, existen exactamente p bucles conjugados en el conjunto $S := \{\beta^y(x) \mid x \in A_p\}$.*

Demostración. Consideremos la siguiente acción

$$\begin{aligned} \phi : \langle y \rangle \times S &\longrightarrow S \\ (y, \beta^y(x)) &\mapsto (\beta^y(x))^y \end{aligned}$$

Se tiene que $\mid Orb(\beta^y(x)) \mid$ es exactamente $\langle y \rangle / \mid Stab_{\langle y \rangle}(\beta^y(x)) \mid$.

Así, si $\beta^y(x)$ no es estable por y-conjugación, se tiene que $Stab_{\langle y \rangle}(\beta^y(x)) = e$ y por lo tanto $\mid Orb(\beta^y(x)) \mid = p$. □

Fijemos ahora un elemento y en un grupo alternado A_n, $n \geq 5$, y consideremos el bucle $B^y(x)$ asociado al elemento x de A_n. Tendremos que

$$B^y(x) := \{E_{k_1}(x, y), ..., E_{k_2-1}(x, y)\},$$

de modo que $E_{k_2}(x, y) = E_{k_1}(x, y)$.

Fijado un elemento z del bucle $B^y(x)$, como $z = [\tau, y]$ para un elemento $\tau \in B^y(x)$, se tiene que $z = [\sigma\tau, y]$ para todo $\sigma \in C_{A_n}(y)$, y por tanto que el conjunto de elementos que conmutados por y dan como resultado z es exactamente

$$A := \{\tau\sigma \mid \sigma \in C_{A_n}(y)\}.$$

Además, sabiendo que tanto z como τ son elementos de $B^y(x)$, se tiene que el único elemento de A que pertenece a $B^y(x)$ es τ. El resto de elementos no pertenece al bucle asociado al elemento x.

De este modo, para cualquier elemento z_1 en un bucle $B^y(x)$, se tiene que hay exactamente un elemento z_2 del bucle que conmutado con y da como resultado z_1 y que hay $\mid C_{A_n}(y) \mid -1$ elementos fuera del bucle $B^y(x)$ que conmutados con y dan como resultado z_1.

Definición 4.3.3. *Fijado un elemento y en un grupo alternado A_n, $n \geq 5$. Se define el Anulador de y como el conjunto de elementos x de A_n verificando que existe un $k \in \mathbb{N}$ tal que $E_k(x, y) = e$. Denotaremos a este conjunto por $\mathcal{T}_y$.*

En definitiva, el Anulador de y no es más que el conjunto de elementos de A_n cuyas cadenas se estacionan en el elemento neutro. Si $\mathcal{C}_y$ define el conjunto de elementos de A_n cuyas cadenas se estacionan en un bucle distinto del elemento neutro, entonces

$$A_n = \mathcal{T}_y \cup \mathcal{C}_y.$$

Además, $\mathcal{C}_y = \cup_{i=0}^{\alpha(y)} \mathcal{C}_y^i$, donde $\mathcal{C}_y^0$ es el conjunto de los elementos distintos del neutro que pertenecen a un bucle $B^y(x)$, $\mathcal{C}_y^1$ es el conjunto de elementos de A_n que no pertenecen a $\mathcal{C}_y^0$, pero que su conmutador por y pertenece a $\mathcal{C}_y^0$ e, inductivamente,

$$\mathcal{C}_y^{i+1} := \{x \in A_n \backslash \mathcal{C}_y^i \mid [x, y] \in \mathcal{C}_y^i\}.$$

Notemos que existirá un índice $\alpha(y) \in \mathbb{N}$ tal que $\mathcal{C}_y^{\alpha(y)+1} = \emptyset$.

Nos planteamos estudiar, usando GAP, la longitud de las cadenas que se estacionan en el elemento neutro para grupos alternados no muy grandes. El algoritmo utilizado fue el siguiente:

```
1: G:=AlternatingGroup(n); # Siendo n el entero que deseemos.
2: y:=..;# Siendo y la permutación de A_n que deseemos.
3: H:=Centralizer(G,y)
4: a:=1; b:=2;
5: B:=[[()]];
6: B[2]:=[];
7: for z in H do
8:     Add(B[2],z);
9: end for
10: Remove(B[2],1);
11: while a>0 do
12:     b:=b+1;
13:     B[b]:=[];
```

```
14:     for x in G do
15:         p:=Comm(x,y);
16:         if p in B[b-1] then
17:             Add(B[b],x);
18:         end if
19:     end for
20:     a:=Length(B[b]);
21: end while
22: Remove(B,b);
23: R:=Length(B);
24: Print("La longitud máxima de las cadenas de T_y es: ", R-1);
```

Usando ese algoritmo para los grupos alternados más pequeños podemos ver que para ciertos órdenes, la longitud de la cadena es 2.

En principio, y para el caso general, no parece existir un medio fácil de saber a priori la longitud máxima de las cadenas de $\mathcal{T}_y$, pero para casos particulares podemos saber cuántos elementos pertenecen a $\mathcal{T}_y$ y qué elementos son. Los resultados obtenidos computacionalmente haciendo uso del algoritmo anterior se recogen en la siguiente tabla:

Grupo alternado	Longitud Máxima	Tiempo de Ejecución
A_5	2	2 mmsec
A_6	2	6 mmsec
A_7	2	21 mmsec
A_8	2	177 mmsec
A_9	3	3 seg 76 mmsec
A_{10}	3	32 seg 605 mmsec
A_{11}	2	4 min 50 seg 635 mmsec
A_{12}	2	57 min 23 seg 380 mmsec
A_{13}	2	16 h 20 min 19 seg
A_{14}	2	$>$ 10 días

Cuadro 4.2: Longitudes de Cadenas estacionadas en el neutro.

Pero para ciertos grupos alternados es posible probar que la longitud de la cadena es siempre 2, lo que se recoge en los siguientes resultados.

Lema 4.3.5. *Consideremos un grupo alternado A_n, $n \geq 5$ e impar, y sea $y = (1, 2, ..., n)$ un ciclo del longitud máxima en A_n. Se tiene que $C_{A_n}(y) = \langle y \rangle$ y que $\mid N_{A_n}(C_{A_n}(y)) \mid$ es ó $n\varphi(n)$ ó $n\varphi(n)/2$, donde φ es la función de Euler.*

Demostración. El número de conjugados de un n-ciclo en S_n es $(1/n)V_n^n = (n-1)!$. Así, $\mid S_n : C_{S_n}(y) \mid = (n-1)!$. Se tiene entonces que

$$\mid C_{S_n}(y) \mid = \frac{\mid S_n \mid}{\mid Cl_{S_n}(y) \mid} = \frac{n!}{(n-1)!} = n.$$

Como $\mid \langle y \rangle \mid = n$, tendremos que $C_{S_n}(y) = \langle y \rangle$. En el grupo $\langle y \rangle$, existen exactamente $\phi(n)$ elementos del mismo tipo que y, por lo que tendremos que $\mid N_{S_n}(\langle y \rangle) \mid = n\varphi(n)$.

Por definición, $N_{A_n}(\langle y \rangle) = \{x \in A_n \mid y^x \in \langle y \rangle\}$. Si para todo i con $mcd(i, n) = 1$ se tiene que los elementos y e y^i son conjugados en A_n, el número de grupos conjugados en A_n al grupo $\langle y \rangle$ sería la mitad del número de grupos conjugados en S_n a dicho grupo, por lo que $N_{A_n}(\langle y \rangle) = N_{S_n}(\langle y \rangle)$ y entonces

$$\mid N_{A_n}(\langle y \rangle) \mid = n\varphi(n).$$

Si la mitad de potencias de y son conjugadas en A_n a y, tendremos que existe $\sigma \in S_n \backslash A_n$ tal que $\sigma \in N_{S_n}(\langle y \rangle)$. De este modo,

$$\mid N_{A_n}(\langle y \rangle) \mid = \frac{\mid N_{S_n}(\langle y \rangle) \mid}{2} = \frac{n\varphi(n)}{2}.$$

□

Lema 4.3.6. *Sea p un número primo mayor que 3. Consideremos y un ciclo de longitud máxima en A_p. El Anulador de y, $\mathcal{T}_y$, en A_p es exactamente el grupo $N_{A_p}(\langle y \rangle)$.*

Demostración. Sea $Z = \langle y \rangle = C_{A_p}(y)$ y $N_1 = N_{A_p}(Z)$. Consideremos $N_2 := \{x \in A_n \mid Z^x \subset N_1\}$ e inductivamente

$$N_r := \{x \in A_n \mid Z^x \subset N_{r-1}\}.$$

Notemos que $E_3(x, y) = 1$ si y sólo si $E_2(E_1(x, y), y) = e$, es decir, $E_1(x, y) \in N_1$. Por tanto, $x^{-1}y^{-1}xy$ es un elemento de N_1 y además, $y \in Z \subset N_1$, luego $(y^{-1})^x$ es un elemento de N_1, es decir, $Z^x \subset N_1$.

Hemos probado que $x \in N_2$ si y sólo si $E_3(x,y) = 1$. Probaremos por inducción que $E_{r+1}(x,y) = 1$ si y sólo si $x \in N_r$.

$E_{r+1}(x,y) = 1$ si y sólo si $E_r(E_1(x,y),y)$ lo que es equivalente (aplicando la hipótesis de inducción) a que $E_1(x,y) \in N_{r-1}$, es decir, $[x,y] \in N_{r-1}$.

Esto implica que $(y^{-1})^x \in N_{r-1}$, es decir, $Z^x \subset N^{r-1}$, y por definición esto es equivalente a decir que $x \in N_r$.

Tenemos entonces dos cadenas:

- $Z \subset N_1 \subset N_2 \subset N_3 \subset ...$
- $Z \subset N_{A_p}(Z) = N_1 \subset N_{A_p}(N_1) = \tilde{N_2} \subset N_{A_p}(N_2) = \tilde{N_3} \subset ...$

Como p es un número primo se tiene que $Z \in Syl_p(A_p)$ y como N_1 es autonormalizante, tendremos que $\tilde{N_2} = N_1$.

Si tomamos x un elemento en N_2 se tiene que $Z^x \subset N_1$ y que además, $Z, Z^x \in Syl_p(N_1)$ lo que implica que $Z = Z^x$ y por tanto $x \in N_1$. Así, tendremos que $N_1 = N_2$.

Como $\mathcal{T}_y = \cup_{i \geq 1} N_i$, se tiene que

$$\mathcal{T}_y = N_1 = N_{A_p}(\langle y \rangle).$$

□

Lema 4.3.7. *Sea n un entero positivo tal que $mcd(n, \varphi(n)) = 1$ e y un n-ciclo en A_n. El Anulador de y, $\mathcal{T}_y$, en A_n es exactamente el grupo $N_{A_n}(\langle y \rangle)$.*

Demostración. Sea p_i un primo divisor de n. Dado $P_i \in Syl_{p_i}(\langle y \rangle)$, se tiene que $P_i \trianglelefteq N_{A_n}(\langle y \rangle)$ y como $mcd(n, \varphi(n)) = 1$ se tiene que $\langle y \rangle$ es el único subgrupo de $N_{A_n}(\langle y \rangle)$ de orden n. Entonces, en vista de los argumentos utilizados en la demostración del lema 4.3.5, se tiene que $N_1 = N_2$. □

El siguiente corolario es inmediato y nos proporciona información sobre la longitud máxima de las cadenas que se estacionan en el elemento neutro bajo las condiciones del del lema 4.3.6.

Corolario 4.3.8. *Sea n un entero positivo tal que $mcd(n, \varphi(n)) = 1$ e y un ciclo de longitud máxima en A_n. Entonces la longitud máxima de una Cadena $E^y(x) \subset \mathcal{T}_y$ que se estaciona en el elemento neutro es* 2.

Demostración. Si $E_m(x,y) = e$ se tiene que $E_{m-1}(x,y) \in \langle y \rangle$. Además, se tiene que $E_{m-2}(x,y) \in N_{A_n}(\langle y \rangle)$.

En vista del lema 4.3.7, tenemos que $N_{A_n}(\langle y \rangle)$ es autonormalizante. Esto implica que la longitud máxima de la cadena es $m - (m-2) = 2$.

□

Como se puede observar, el último corolario concuerda perfectamente con los resultados obtenidos de manera computacional expuestos en la Tabla 4.2. Si nos fijamos en dicha tabla, para los grupos alternados A_9 y A_{10}, se obtuvo computacionalmente que la longitud máxima de las cadenas que se estacionan en el neutro es 3. Se tiene que para $n = 9, 10$, $\varphi(9) = 6$ y $\varphi(10) = 4$, por lo que $mcd(n, \varphi(n)) \neq 1$.

Se ve además, que las hipótesis del corolario 4.3.8 son condiciones suficientes pero no necesarias, puesto que para $n = 8$ y $n = 12$ se obtuvo computacionalmente que la longitud máxima de las cadenas que se estacionan en el neutro es 2 y además, en ambos casos, $mcd(n, \varphi(n)) \neq 1$.

Capítulo 5

El grupo de Nottingham y su álgebra de Lie

En 1896 Frobenius empezó a usar la Teoría de Caracteres para estudiar las soluciones de ecuaciones en grupos. En [5] construyó un fórmula para calcular, fijado un elemento g en un grupo finito G, el número de soluciones de la ecuación

$$[x, y] = g.$$

Más de cien años después, en 2010, Liebeck, O'Brian, Shalev y Tiep ([16]) hicieron uso de la fórmula proporcionada por Frobenius para probar la Conjetura de Ore en muchos Grupos Simples.

Dada una palabra ω, se dice que ω tiene anchura finita en G si todo elemento del subgrupo verbal $\omega(G)$ se puede expresar como pruducto de a lo sumo k ω-valores en G o sus inversos. Es decir, cualquier producto de longitud arbitraria de ω-valores en G o sus inversos admite una expresión de longitud acotada por k factores.

Desde mediados del siglo XX han surgido preguntas relativas al comportamiento de los subgrupos verbales. ¿Podemos encontrar una función natural f donde la anchura de ω en cualquier grupo finito G esté acotada superiormente por $f(d(G))$? Aquí $d(G)$ denotará el menor tamaño posible de un conjunto generador.

Si esa función existe, se dice que la palabra ω es uniformemente elíptica sobre los grupos finitos.

En [29] pueden encontrarse respuestas a la pregunta anterior. Además, se plantea dicha en el contexto de grupos profinitos. Este problema, planteado por primera vez por Brian Hartley en [7] tiende un puente entre álgebra y topología, probando que una palabra ω tiene anchura finita en un grupo profinito G si y sólo si el subgrupo verbal $\omega(G)$ es cerrado en G.

Dada una palabra ω, Philip Hall llamó grupo G ω-elíptico si ω tiene anchura finita en G y se dirá que es verbalmente elíptico si G es elíptico

para toda palabra ω. En esta linea, uno de los resultados más profundos fue obtenido por P. Stroud en su tesis doctoral [30] dónde se prueba que todo grupo finitamente generado abeliano por nilpotente es verbalmente elíptico.

En 1996, C. Martínez y E. Zelmanov [22] y en 1997, J. Salx y J. S. Wilson [27], probaron, independientemente, que para todo grupo simple finito suficientemente grande se puede encontrar una constante k para la cual se verifica que $\xi(G)^k = G$. De estos resultados se sigue que la palabra $\omega = x^n$ es elíptica sobre cualquier grupo simple, finito y suficientemente grande G.

Numerosas contribuciones se han hecho desde que se iniciara el estudio de los subgrupos verbales. En [29] se prueba que toda palabra ω tiene anchura finita en en un grupo finito G. Más aun, se sabe que la anchura verbal de ω sobre G estará acotada superiormente por $\mid G \mid$. De esta manera la pregunta sobre si los grupos finitos son ω-elípticos queda resuelta.

Otro resultado en esta línea (ver [29]) nos dice que dado un grupo G y un subgrupo normal nilpotente minimax $N \trianglelefteq G$ tales que G/N es virtualmente abeliano entonces G es verbalmente elíptico.

En el estudio de la anchura verbal sobre grupos infinitos ha habido también algunos avances. Uno de los primeros pasos fue probado por Romankov (véase [25]) quién probó que todo grupo finitamente generado virtualmente nilpotente es verbalmente elíptico.

Si definimos rango (de Prüfer) de un grupo G como

$$rk(G) := sup\{d(H) \mid H \quad \text{es un subgrupo finitamente generado de } G\},$$

se puede deducir un resultado algo más general (ver [29]) a partir del teorema de Romankov: Todo grupo virtualmente nilpotente y de rango finito es verbalmente elíptico. En estos dos resultados se estudia por primera vez la anchura verbal en grupos infinitos.

Cabe preguntarse entonces si existe alguna palabra (no trivial) que posea anchura finita en todo grupo G. La respuesta a esta pregunta se debe a Akbar Rhemtulla quien en [24] prueba explicitamente que una palabra ω del grupo libre $\mathcal{F}_k$ tiene anchura finita sobre todo grupo G si y sólo si existen enteros $e_1, ..., e_k$ tales que $mcd(e_1, ..., e_k) = 1$ y que

$$\omega \in x_1^{e_1} ... x_k^{e_k} \mathcal{F}_k'.$$

El objetivo de este capítulo será probar que el Grupo de Nottingham en característica 0 es verbalmente elíptico. Para ello explotaremos la conexión que existe en entre este grupo y el álgebra de Witt.

A este fin, se introducirán los conceptos análogos en álgebras, se considerarán anchuras verbales y se probará que toda palabra ω es elíptica sobre el álgebra de Witt y posteriormente sobre el grupo de Nottingham.

5.1. Linearizaciones completas de polinomios

En esta primera sección recordaremos la existencia de alguna identidad en un álgebra $\mathcal{A}$ implica también la existencia de alguna identidad multilineal. Para ello comenzaremos recordando la noción de identidad y recordaremos el proceso de linearización completa. Pueden verse los detalles en [33].

Sea ϕ un anillo asociativo conmutativo con identidad. Fijemos un conjunto de símbolos $X := \{x_1, x_2, x_3...\}$ y $f = f(x_1, ..., x_n)$ un polinomio no asociativo de $\phi[X]$.

Definición 5.1.1. *Sea $\mathcal{A}$ una ϕ-ágebra. El polinomio no asociativo $f = f(x_1, ..., x_n)$ de $\phi[X]$ se dice que es una identidad en la ϕ-álgebra $\mathcal{A}$ si*

$$f(a_1, ..., a_n) = 0$$

para cualesquiera $a_1, ..., a_n \in \mathcal{A}$. Se dice también que $\mathcal{A}$ satisface la identidad f.

La colección de todas las identidades que se satisfacen en una ϕ-álgebra dada $\mathcal{A}$ es un ideal del álgebra $\phi[X]$, que se llama ideal de identidades y se denota por $\mathcal{T}(\mathcal{A})$.

Un ejemplo sencillo se obtiene considerando una ϕ-álgebra de Lie $\mathcal{L}$, para la cual los polinomios $f_1(x_1) = x_1^2$ y $f_2(x_1, x_2, x_3) = (x_1x_2)x_3 + (x_2x_3)x_1 + (x_3x_1)x_2$ son identidades de $\mathcal{L}$.

Podemos descomponer todo polinomio no asociativo f en $\phi[X]$ de manera única como suma de monomios. Diremos que un monomio αv, con $\alpha \in \phi$ y v una palabra no asociativa, posee tipo $[n_1, ..., n_k]$ si la palabra v contiene a x_i exactamente n_i veces y además, $n_k \neq 0$ pero $n_j = 0$ para todo $j \geq k$.

Llamaremos a n_i el grado del monomio αv en x_i.

Definición 5.1.2. *Sea f un polinomio no asociativo en $\phi[X]$. Si todos los monomios de la descomposición de f tienen el mismo grado n_i en x_i, diremos que f es un polinomio homogéneo en x_i de grado n_i. El polinomio f se dirá homogéneo si es homogéneo en todas las variables.*

Por ejemplo, el polinomio

$$f(x_1, ..., x_4) = (x_1^2x_2)x_4 + ((x_1x_4)x_2)x_1 + (x_1x_4)(x_2x_1)$$

es un polinomio homogéneo ya que cada monomio sumando suyo es de tipo $[2, 1, 0, 1]$.

Definición 5.1.3. *Un monomio no asociativo f en $\phi[X]$ se dirá multilineal si es de tipo $[n_1, ..., n_k]$, con $n_i \leq 1$ para todo $i \in \{1, ..., k\}$. Un polinomio no asociativo se dirá multilineal si cada monomio sumando suyo es multilineal. El grado de un polinomio no asociativo f en x_i se define como el grado máximo en x_i de todos sus monomios.*

Consideremos ahora un polinomio no asociativo f en $\phi[X]$. Si agrupamos todos los monomios del mismo tipo juntos tendremos que f puede ser representado como suma de polinomios homogéneos. Cada uno de estos polinomios homogéneos se llama componente homogénea del polinomio f.

Tomemos $y_1, ..., y_k$ elementos en $\phi[X]\backslash\{x_1, ..., x_n\}$. Para cada $i \in \{1, 2, ..., n\}$ definiremos el polinomio no asociativo fL_i^k mediante la fórmula siguiente.

$$fL_i^k(x_1, ..., x_{i-1}, y_1, ..., y_k, x_{i+1}, ..., x_n) =$$

$$f(x_1, ..., x_{i-1}, y_1 + ... + y_k, x_{i+1}, ..., x_n)$$

$$- \sum_{q=1}^{k} f(x_1, ..., x_{i-1}, y_1 + ... + \widehat{y_q} + ... + y_k, x_{i+1}, ..., x_n)$$

$$+ \sum_{1 \leq q_1 \leq q_2 \leq k} f(x_1, ..., x_{i-1}, y_1 + ... + \widehat{y_{q_1}} + ... + \widehat{y_{q_1}} + ... + y_k, x_{i+1}, ..., x_n)$$

$$-... + (-1)^{k-1} \sum_{q=1}^{k} f(x_1, ..., x_{i-1}, y_q, x_{i+1}, ..., x_n).$$

A la vista de la fórmula anterior, el siguiente resultado es obvio.

Lema 5.1.1. *Sea P un subsemigrupo y Q un subgrupo del grupo aditivo de la ϕ-álgebra $\mathcal{A}$. Si para un polinomio no asociativo $f = f(x_1, ..., x_n)$ y cualquier conjunto de elementos $\{a_1, ..., a_n\} \subset P$ se tiene que $f(a_1, ..., a_n) \in Q$ entonces para cualquier conjunto de elementos $\{a_1, ..., a_{i-1}, b_1, ..., b_k, a_{i+1}, ..., a_n\} \subset P$ se verificará que*

$$fL_i^k(a_1, ..., a_{i-1}, b_1, ..., b_k, a_{i+1}, ..., a_n) \in Q.$$

En particular, si f es una identidad en $\mathcal{A}$, se tiene que fL_i^k también lo será.

Por tanto, el operador L_i^k transforma una identidad del álgebra $\mathcal{A}$ en otra identidad del álgebra $\mathcal{A}$.

Lema 5.1.2. *Sea $g : \mathcal{A} \times ... \times \mathcal{A} \longrightarrow \mathcal{A}$ una función de n variables definida sobre la ϕ-álgebra $\mathcal{A}$ y lineal en cada argumento. Entonces para cualesquiera*

elementos $a_1, a_2, ..., a_k \in \mathcal{A}$*, dónde* $k \geq n$ *se tiene que*

$$g(a_1 + a_2 + ... + a_k, ..., a_1 + a_2 + ... + a_k)$$

$$- \sum_{q=1}^{k} g(a_1 + ... + \widehat{a_q} + ... + a_k, ..., a_1 + ... + \widehat{a_q} + ... + a_k)$$

$$+ \sum_{1 \leq q_1 < q_2 \leq k} g(a_1 + ... + \widehat{a_{q_1}} + ... + \widehat{a_{q_2}} + ... + a_k, ...,$$

$$a_1 + ... + \widehat{a_{q_1}} + ... + \widehat{a_{q_2}} + ... + a_k) + ... + (-1)^{k-1} \sum_{q=1}^{k} g(a_q, ..., a_q) =$$

$$= \begin{cases} \sum_{\sigma \in S_n} g(a_{\sigma(1)}, a_{\sigma(2)}, ..., a_{\sigma(n)}), & si\ k = n \\ 0, & si\ k > n. \end{cases}$$

Demostración. Consideremos $k \geq n$. Debido a que la función g es lineal en cada argumento, podemos convertir todos los sumandos en las variables en sumandos de la función.

Si hacemos esto, el lado izquierdo de la igualdad es una combinación lineal de elementos de la forma $g(a_{j_1}, a_{j_2}, ..., a_{j_n})$ con coeficientes enteros.

Si nos encontramos s índices distintos entre $j_1, ..., j_n$ y s es menor que k, entonces el coeficiente para $g(a_{j_1}, a_{j_2}, ..., a_{j_n})$ es exactamente la suma alternada

$$1 - \binom{k-s}{1} + \binom{k-s}{2} - ... + (-1)^{k-2} \binom{k-s}{k-s}$$

que es igual a 0.

Si $s \geq k$ sólo puede ocurrir que $s = k = n$. En este caso el coeficiente para $g(a_{j_1}, a_{j_2}, ..., a_{j_n})$ a la vista de la fórmula anterior es claramente 1, lo que prueba el lema. □

Lema 5.1.3. *Para cualesquiera* $f, f' \in \phi[X]$ *en los que el operador* L_i^k *esté definido se tiene que* $(f + f')L_i^k = fL_i^k + f'L_i^k$*. Si* $f(x_1, x_2, ..., x_m)$ *es un monomio de grado* n *en* x_i *y* $g := g(x_1, ..., x_{i-1}, y_1, ..., y_n, x_{i+1}, ..., x_m)$ *es un monomio lineal en* $y_1, ..., y_n \in X \setminus \{x_1, ..., x_m\}$ *verificando que* $f(x_1, ..., x_m) = g(x_1, ..., x_{i-1}, x_i, ..., x_i, x_{i+1}, ..., x_m)$*, entonces*

$$fL_i^k(x_1, ..., x_{i-1}, z_1, ..., z_k, x_{i+1}, ..., x_m)$$

$$= \begin{cases} \sum_{\sigma \in S_n} g(x_1, ..., x_{i-1}, z_{\sigma(1)}, ..., z_{\sigma(k)}, x_{i+1}, ..., x_m), & si\ k = n \\ 0, \quad si\ k > n. \end{cases}$$

Demostración. La linearidad del operador L_i^k se sigue directamente de la definición. Si f y g son los monomios indicados en las hipótesis del lema,

fijado $x_1, ..., x_{i-1}, x_{i+1}, ..., x_m$ podemos considerar el monomio g como una función de n variables y aplicar el lema 5.1.2 para obtener el resultado. □

Veamos un ejemplo del uso del último resultado.

$$\begin{aligned}[x_1^2(x_2x_1)]L_1^3 &= (y_1y_2)(x_2y_3) + (y_2y_1)(x_2y_3) + (y_1y_3)(x_2y_2) \\ &+ (y_3y_1)(x_2y_2) + (y_2y_3)(x_2y_1) + (y_3y_2)(x_2y_1).\end{aligned}$$

Definición 5.1.4. *Sea $f = f(x_1, ..., x_n)$ un polinomio homogéneo de tipo $[k_1, ..., k_n]$. El polinomio multilineal $fL_1^{k_1}L_2^{k_2}...L_n^{k_n}$ se denomina linearización completa del polinomio f.*

Lema 5.1.4. *Consideremos $f = f(x_1, ..., x_n)$ un polinomio no asociativo que se anula sobre cualquier sustitución de elementos de un subgrupo P del grupo aditivo de la ϕ-álgebra $\mathcal{A}$. Entonces la linearización completa de cualquiera de sus componentes homogéneas de grado máximo también se anula en $\mathcal{A}$.*

Demostración. Consideremos la descomposición de f en la suma de sus componentes homogéneas $f_1 + ... + f_s$ y consideremos, sin pérdida de generalidad, que el grado de f_1 es maximal.

Supongamos que alguna variable x_j no aparece en f_1 pero si que aparece en alguna otra componente homogénea de f. Entonces el polinomio

$$f'(x_1, ..., x_n) = f(x_1, ..., x_{j-1}, 0, x_{j+1}, ..., x_n),$$

también se anula sobre P, tiene a f_1 como componente homogénea de grado maximal y además, f' no contiene la variable x_j.

Por otro lado, si x_j aparece en f_1 pero no aparece en alguna otra componente homogénea del polinomio f' podemos considerar el nuevo polinomio

$$f''(x_1, ..., x_n) = f'(x_1, ..., x_n) - f'(x_1, ..., x_{j-1}, 0, x_{j+1}, ..., x_n).$$

El polinomio f'' también se anula sobre P, pero ahora x_j aparece en todas las componentes homogéneas de f'' y, como antes, tiene a f_1 como componente homogénea de grado maximal.

De este modo, renombrando las variables si fuese necesario, podemos asumir que la componente homogénea f_1 del polinomio f tiene tipo $[k_1, ..., k_n]$, dónde $k_i \neq 0$ para todo $i = 1, ..., n$. Además, las componentes homogéneas restantes (pongamos por ejemplo f_2) tendrán tipo $[m_1, ..., m_n]$, con $m_i \neq 0$ para todo $i = 1, ..., n$ y donde además, la desigualdad $m_j < k_j$ se cumple para algún $j \in \{1, ..., n\}$.

Como $m_j < k_j$, entonces $f_2 L_1^{k_1} L_2^{k_2} ... L_n^{k_n} = 0$ gracias al lema 5.1.3. De este modo, tendremos que

$$f L_1^{k_1} L_2^{k_2} ... L_n^{k_n} = f_1 L_1^{k_1} L_2^{k_2} ... L_n^{k_n}.$$

Gracias al lema 5.1.1 podemos concluir que la linearización Completa de f_1 se anula sobre P. □

Con todo lo hecho hasta el momento, podemos enunciar el resultado principal de esta sección.

Teorema 5.1.5. *Si una ϕ-álgebra $\mathcal{A}$ satisface alguna identidad, entonces también satisface alguna identidad multilineal.*

5.2. Anchuras verbales sobre álgebras

En esta sección consideraremos anchuras verbales de polinomios sobre álgebras. Particularizaremos algunos resultados en el álgebra de matrices $M_n(\mathbb{F})$ y en el álgebra de Virasoro.

Consideremos un álgebra $\mathcal{A}$ sobre el anillo ϕ y tomemos un polinomio $f = f(x_1, .., x_n)$ en $\phi[X]$.

Definición 5.2.1. *Consideremos $sp_\phi(f(\mathcal{A}))$ la clausura lineal del conjunto de valores de $f(\mathcal{A})$. Se define la anchura verbal del polinomio f como el mínimo $m \in \mathbb{N}$ verificando que todo elemento $a \in sp_\phi(f(\mathcal{A}))$ puede escribirse como suma de m valores de f en $\mathcal{A}$*

$$a = f(x_1^{(1)}, ..., x_n^{(1)}) + ... + f(x_1^{(m)}, ..., x_n^{(m)}),$$

con $x_i^{(j)} \in \mathcal{A}$ para todo $i \in \{1, ..., n\}$ y para todo $j \in \{1, ..., m\}$.

Se dirá que la anchura verbal del polinomio f sobre A es $\omega_\mathcal{A}(f) = m$.

El objetivo de las siguientes lineas es estudiar la anchura verbal de monomios y de sus linearizaciones completas cuando ϕ es un cuerpo.

Lema 5.2.1. *Sea $\mathbb{F}$ un cuerpo de característica 0 , $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ y f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Si tomamos $g := f L_i^{k_i}$ la linearización completa del polinomio f en la variable x_i tendremos que $sp_\mathbb{F}(g(\mathcal{A})) \subset sp_\mathbb{F}(f(\mathcal{A}))$.*

Demostración. Debido a la construcción de g, se tiene que

$$f L_i^{k_i}(x_1, ..., x_{i-1}, y_1, ..., y_{k_i}, x_{i+1}, ..., x_n)$$

será igual a

$$\begin{gathered} f(x_1,...,x_{i-1},y_1+...+y_{k_i},x_{i+1},...,x_n) \\ -\sum_{q=1}^{k_i} f(x_1,...,x_{i-1},y_1+...+\widehat{y_q}+...+y_{k_i},x_{i+1},...,x_n) \\ +\sum_{1\leq q_1\leq q_2\leq k_i} f(x_1,...,x_{i-1},y_1+...+\widehat{y_{q_1}}+...+\widehat{y_{q_1}}+...+y_{k_i},x_{i+1},...,x_n) \\ -...+(-1)^{k_i-1}\sum_{q=1}^{k_i} f(x_1,...,x_{i-1},y_q,x_{i+1},...,x_n). \end{gathered}$$

Acorde a la expresión anterior, si un elemento $a \in sp_{\mathbb{F}}(g(\mathcal{A}))$ entonces se podrá expresar como suma de evaluaciones del polinomio f sobre el álgebra $\mathcal{A}$, de dónde se sigue el resultado. □

Ahora generalizaremos el resultado anterior para el caso en el que consideremos linearizaciones completas de monomios.

Teorema 5.2.2. *Sea $\mathbb{F}$ un cuerpo de característica 0 , $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ y f un monomio de tipo $[k_1,...,k_n]$ en $\mathbb{F}[X]$. Si h es la linearización completa de f entonces $sp_{\mathbb{F}}(f(\mathcal{A})) = sp_{\mathbb{F}}(h(\mathcal{A}))$.*

Demostración. Como $h = fL_1^{k_1}...L_n^{k_n}(x_{11},...,x_{1k_1},...,x_{n1},...,x_{nk_n})$ y se tiene que esta expresión es igual a

$$\sum_{\pi_1\in S_{k_1}} ... \sum_{\pi_n\in S_{k_n}} g(x_{11},...,x_{1k_1},...,x_{n1},...,x_{nk_n}),$$

donde se verifica que la función g verifica que

$$g(x_1,...,x_1,...,x_n,...,x_n) = f(x_1,...,x_n).$$

Tendremos que

$$h(x_1,...,x_1,...,x_n,...,x_n) = (k_1!...k_n!)f(x_1,...,x_n),$$

y como estamos trabajando en un cuerpo de característica 0, se tiene que $0 \neq (k_1!...k_n!)^{-1}$.

Por lo tanto, todo elemento de $sp_{\mathbb{F}}(f(\mathcal{A}))$ puede escribirse como un elemento de $sp_{\mathbb{F}}(h(\mathcal{A}))$.

Para ver el otro contenido, basta aplicar el lema 5.2.1 n veces, una por variable, para obtener que

$$sp_{\mathbb{F}}(fL_1^{k_1}...L_n^{k_n}(\mathcal{A})) \subset sp_{\mathbb{F}}(f(\mathcal{A})).$$

□

Debido a la linearidad de los operadores $L_i^{k_i}$ el resultado anterior se extiende automáticamente para polinomios homogéneos.

Corolario 5.2.3. *Sea $\mathbb{F}$ un cuerpo de característica 0 , $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ y f un polinomio homogéneo de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Si h es la linearización completa de f entonces $sp_{\mathbb{F}}(f(\mathcal{A})) = sp_{\mathbb{F}}(h(\mathcal{A}))$.*

De manera inmediata se puede probar el siguiente resultado.

Corolario 5.2.4. *Sea $\mathbb{F}$ un cuerpo de característica 0 , $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ con identidad y f un polinomio homogéneo de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Si h es la linearización completa de f entonces $sp_{\mathbb{F}}(f(\mathcal{A})) = sp_{\mathbb{F}}(h(\mathcal{A})) = \mathcal{A}$.*

Demostración. Basta darse cuenta de que para todo $a \in \mathcal{A}$, se tiene que $h(a, 1, ..., 1) = \beta a$ para cierto $\beta \in \mathbb{F}$ dependiente del número de componentes homogéneas de f así como del coeficiente de las mismas.

Como h es multilineal y (F) es un cuerpo de característica 0, es posible considerar $b = 1/\beta a$ y obtener que, $h(b, 1, ..., 1) = a$.

Así, para todo $a \in \mathcal{A}$ se tiene que $a \in sp_{\mathbb{F}}(h(\mathcal{A})) \subset \mathcal{A}$, de donde se sigue el resultado. □

Una vez se ha probado que la clausura lineal de las imágenes de un polinomio homogéneo f sobre álgebra $\mathcal{A}$ (en característica 0), coinciden con las imágenes de la linearización completa de f sobre el álgebra $\mathcal{A}$, podemos plantearnos la comparación de las anchuras verbales del polinomio f y de su linearización completa h sobre el álgebra $\mathcal{A}$.

Lema 5.2.5. *Sea $\mathbb{F}$ un cuerpo de característica 0 y algebraicamente cerrado. Sea f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Sea $\mathcal{A}$ un álgebra sobre $\mathbb{F}$. Entonces, si h es la linearización completa de f, se tiene que $1 \leq \omega_{\mathcal{A}}(h) \leq \omega_{\mathcal{A}}(f) \leq dim_{\mathbb{F}}\mathcal{A}$.*

Demostración. Basta ver que si el cuerpo $\mathbb{F}$ tiene característica 0, se tiene que $f(\mathcal{A}) \subset g(\mathcal{A})$, puesto que todo elemento

$$a = f(a_1, ..., a_n) = (k_1!...k_n!)^{-1} h(\underbrace{x_1, ..., x_1}_{k_1}, ..., \underbrace{x_n, ..., x_n}_{k_n}).$$

De aquí, usando la miltilinealidad de h se sigue que $\omega_{\mathcal{A}}(h) \leq \omega_{\mathcal{A}}(f)$.

Para ver que $\omega_{\mathcal{A}}(f) \leq dim_{\mathbb{F}}\mathcal{A}$, basta darse cuenta que $f(\mathcal{A})$ genera linealmente $sp_{\mathbb{F}}(f(\mathcal{A}))$ que es un subespacio vectorial de $\mathcal{A}$, por lo que la dimensión de $sp_{\mathbb{F}}(f(\mathcal{A}))$ es siempre menor o igual que la dimensión de $\mathcal{A}$.

Así, todo elemento $a \in sp_{\mathbb{F}}(f(\mathcal{A}))$ puede expresarse como combinación lineal de a lo sumo, $dim_{\mathbb{F}}(\mathcal{A})$ elementos de $f(\mathcal{A})$. Como el cuerpo es algebraicamente cerrado y $\mathbb{F} \subset Z(\mathcal{A})$, siempre es posible sacar raíces a los coeficientes de la combinación lineal e introducirlos en los coeficientes del polinomio.

□

Lema 5.2.6. *Sea $\mathbb{F}$ un cuerpo de caracteristica 0 y f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Sea $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ con identidad. Entonces, si h es la linearización completa de f, se tiene que $1 = \omega_{\mathcal{A}}(h)$.*

Demostración. Para todo $a \in sp_{\mathbb{F}}(h(\mathcal{A}))$, se tiene que $a = h(a, 1, ..., 1)$. □

Lema 5.2.7. *Sea $\mathbb{F}$ un cuerpo de característica 0, f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$ y $\mathcal{A}$ un álgebra sobre $\mathbb{F}$. Entonces, si h es la linearización completa de f, se tiene que*

$$1 \leq \omega_{\mathcal{A}}(h) \leq \omega_{\mathcal{A}}(f) \leq \xi\omega_{\mathcal{A}}(h),$$

donde $\xi = (2^{k_1} - 1)...(2^{k_n} - 1)$.

Demostración. La primera desigualdad se sigue directamente de 5.2.5. Para ver la segunda desigualdad hay que darse cuenta de que $fL_i^{k^i}$ se escribe como:

$$\begin{gathered} f(x_1, ..., x_{i-1}, y_1 + ... + y_{k_i}, x_{i+1}, ..., x_n) \\ - \sum_{q=1}^{k_i} f(x_1, ..., x_{i-1}, y_1 + ... + \widehat{y_q} + ... + y_{k_i}, x_{i+1}, ..., x_n) \\ + \sum_{1 \leq q_1 \leq q_2 \leq k_i} f(x_1, ..., x_{i-1}, y_1 + ... + \widehat{y_{q_1}} + ... + \widehat{y_{q_1}} + ... + y_{k_i}, x_{i+1}, ..., x_n) \\ -... + (-1)^{k_i - 1} \sum_{q=1}^{k_i} f(x_1, ..., x_{i-1}, y_q, x_{i+1}, ..., x_n). \end{gathered}$$

De este modo, y teniendo en cuenta que $h = fL_1^{k_1}...L_n^{k_n}$, se tiene que todo elemento en $h(\mathcal{A})$, se puede escribir como suma de ξ elementos de $f(\mathcal{A})$ de dónde se sigue el resultado. □

Ahora extenderemos los resultados anteriores para el caso de polinomios homogéneos de tipo $[k_1, .., k_n]$.

Consideremos entonces un cuerpo $\mathbb{F}$ y un conjunto de símbolos $X = \{x_1, x_2, x_3, ...\}$. Sea $f = f(x_1, ..., x_n) \in \mathbb{F}[X]$ un polinomio. Se dirá que f es homogéneo de tipo $[k_1, ..., k_n]$ si f se expresa como suma de monomios $f_1, ..., f_n \in \mathbb{F}$, siendo cada monomio de tipo $[k_1, ..., k_n]$.

Sea $f \in \mathbb{F}[X]$ un polinomio no asociativo. Podemos agrupar juntos todos los monomios del mismo tipo de f. Tendremos que f se podrá representar como suma de polinomios homogéneos $g_1, ..., g_r \in \mathbb{F}$. A estos polinomios los llamaremos componentes homogéneas de f.

Lema 5.2.8. *Sea $\mathbb{F}$ un cuerpo de característica 0 y algebraicamente cerrado. Sea f un polinomio homogéneo de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Sea $\mathcal{A}$ un álgebra sobre $\mathbb{F}$. Entonces, si h es la linearización completa de f, se tiene que $1 \leq \omega_{\mathcal{A}}(h) \leq \omega_{\mathcal{A}}(f) \leq dim_{\mathbb{F}}\mathcal{A}$.*

Demostración. Como f es un polinómio homogéneo de tipo $[k_1, ..., k_n]$, se tiene que $f = f_1 + ... + f_t$ para ciertos monomios $f_i = f_i(x_1, ..., x_n) \in \mathbb{F}[X]$ de tipo $[k_1, ..., k_n]$.

Como los operadores $L_i^{k_i}$ son lineales, tendremos que si h es la linearización completa de f entonces

$$h(x_{11}, ..., x_{1k_n}, ..., x_{n1}, ..., x_{nkn}) =$$
$$\sum_{i=1}^{t} f_i L_1^{k_1} ... L_n^{k_n}(x_{11}, ..., x_{1k_n}, ..., x_{n1}, ..., x_{nkn}) =$$
$$\sum_{i=1}^{t} h_i(x_{11}, ..., x_{1k_n}, ..., x_{n1}, ..., x_{nkn}),$$

en dónde cada h_i es la linearización completa del monomio f_i.

Como para cada $i \in \{1, ..., t\}$ se tiene que $f_i(\mathcal{A}) \subset h_i(\mathcal{A})$. Lo que en en particular nos lleva a que $f(\mathcal{A}) \subset h(\mathcal{A})$. Aplicando ahora el mismo argumento que en el lema 5.2.5 se obtiene el resultado. □

Lema 5.2.9. *Sea $\mathbb{F}$ un cuerpo de característica 0 y f un polinomio homogéneo de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Sea $\mathcal{A}$ un álgebra sobre $\mathbb{F}$ con identidad. Entonces, si h es la linearización completa de f, se tiene que $1 = \omega_{\mathcal{A}}(h)$.*

Demostración. Para todo $a \in sp_{\mathbb{F}}(h(\mathcal{A}))$ se tiene que $h(a, 1, ..., 1) = \lambda a$ para cierto $\lambda \in \mathbb{F}$ (dependiente del número de componentes homogéneas de f y de los coeficientes de las mismas).

Basta recordar que h es multilineal para obtener el resultado. □

5.2.1. El álgebra de matrices $M_n(\mathbb{F})$

Estudiaremos, a modo de ejemplo, la anchura verbal en un álgebra muy particular, el álgebra de matrices $M_n(\mathbb{F})$, con $\mathbb{F}$ un cuerpo de característica 0.

Lema 5.2.10. *Sea $\mathbb{F}$ un cuerpo de característica 0 y f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$. Entonces,*

$$sp_{\mathbb{F}}(f(M_n(\mathbb{F}))) = M_n(\mathbb{F}).$$

Demostración. Consideremos la primera variable que aparece en la expresión de f. Sin pérdida de generalidad podemos suponer que es x_1.

Consideremos $\{e_{ij} \mid i, j \in \{1, ..., n\}\}$ la base usual de $M_n(\mathbb{F})$. Se tiene que para todo $i \in \{1, .., n\}$ se verifica que $f(e_{ii}, Id, ..., Id) = e_{ii}$, puesto que e_{ii} es idempotente para todo i. Entonces $e_{ii} \in sp_{\mathbb{F}}(f(M_n(\mathbb{F})))$ para todo i.

Para ver e_{ij} con $i \neq j$ está también en $sp_{\mathbb{F}}(f(M_n(\mathbb{F})))$ basta con observar la expresión

$$f((e_{ii} + e_{ij}), Id, ..., Id) = (e_{ii} + e_{ij})^{k_1}.$$

Como e_{ii} es idemponente, e_{ij} es nilpotente de grado 2, $e_{ij}e_{ii} = 0$ y $e_{ii}e_{ij} = e_{ij}$ tendremos que

$$(e_{ii} + e_{ij})^{k_1} = e_{ii} + \lambda e_{ij},$$

para cierto $\lambda \in \mathbb{Z}\backslash\{0\}$.

Como $\mathbb{F}$ tiene característica 0, podemos encontrar el inverso de λ para obtener que $\{e_{ij} \mid i, j \in \{1, ..., n\}\} \subset sp_{\mathbb{F}}(f(M_n(\mathbb{F})))$, de dónde se sigue el resultado. □

Ahora pasamos a estudiar la anchura verbal de monomios sobre $M_2(\mathbb{F})$, con $\mathbb{F}$ un cuerpo de característica 0.

Teorema 5.2.11. *Sea $\mathbb{F}$ un cuerpo algebraicamente cerrado de característica 0. Sea f un monomio de tipo $[k_1, ..., k_n]$ en $\mathbb{F}[X]$ y sea h su linearización completa. Entonces*

$$1 = \omega_{M_2(\mathbb{F})}(h) \leq \omega_{M_2(\mathbb{F})}(f) \leq 2.$$

Demostración. La primera igualdad se sigue del lema 5.2.6.

Para cada matriz $A \in M_2(\mathbb{F})$ se pueden encontrar dos matrices $A_1, A_2 \in M_2(\mathbb{F})$ (dependientes de A) de modo que $A = A_1 + (A_2)^{k_1}$, con A_1 idempotente y A_2 diagonal.

Entonces para todo monomio $f = f(x_1, ..., x_n)$ de tipo $[k_1, ..., k_n]$ tendremos que

$$f(A_1, Id, ..., Id) = \alpha(A_1)^{k_1} = \alpha A_1 \quad f(A_2, Id, ..., Id) = \alpha(A_2)^{k_1},$$

para algún $\alpha \in \mathbb{F}$.

De este modo, tendremos que

$$f(A_1, Id, ..., Id) + f(A_2, Id, ..., Id) = \alpha(A_1 + A_2^{k_1}).$$

Basta escoger $B_1 = 1/\alpha^{1/k_1} A_1$ y $B_2 = ((1/\alpha)A_2)^{1/k_1}$, lo que es posible puesto que el cuerpo $\mathbb{F}$ es algebraicamente cerrado y de característica 0 y la matriz A_2 es diagonal.

Así, tendremos que

$$f(B_1, Id, ..., Id) + f(B_2, Id, ..., Id) = A_1 + A_2 = A.$$

□

Hemos visto que la anchura verbal de un monomio f de tipo $[k_1, ..., k_n]$ sobre un cuerpo de característica 0 y algebraicamente cerrado en el álgebra de matrices sobre ese cuerpo es o bien 1 o bien 2, dependiendo del monomio considerado.

Si k_i es igual a 1 para algún $i \in \{1, ..., n\}$, es claro que $\omega_{M_2(\mathbb{F})}(f) = 1$.

También hay monomios para los que la anchura es 2. Si el cuerpo con el que trabajamos no es algebraicamente cerrado, por ejemplo el cuerpo de los números racionales $\mathbb{Q}$, y tomamos una matriz $A \in M_2(\mathbb{Q})$ cuyo determinante sea -1, para el polinomio $f = x^2$ no puede existir ninguna matriz $B \in M_2(\mathbb{Q})$ tal que $B^2 = A$. Por tanto, la anchura sería estrictamente mayor que 1 para f.

5.3. El álgebra de Virasoro

En esta sección se hará un estudio del Álgebra de Virasoro, $\mathcal{V}ir$, así como de algunas de sus subálgebras, el álgebra de Witt, W_1, el álgebra W_0 y el álgebra W_0^+, que se utilizarán en secciones posteriores. $\mathbb{F}$ será un cuerpo de característica 0. El *Álgebra de Virasoro* sin centro, $\mathcal{V}ir$, tiene una base $\{e_i \mid i \in \mathbb{Z}\}$ con la multiplicación dada por $[e_i, e_j] = (i - j)e_{i+j}$. Es decir, se tiene que

$$\mathcal{V}ir := \bigoplus_{n\mathbb{Z}} \mathbb{F}e_n.$$

Las subálgebras W_1, W_0 y W_0^+ vienen dadas por las siguientes expresiones:

$$W_1 := \bigoplus_{i \geq -1} \mathbb{F}e_i, \quad W_0 := \bigoplus_{i \geq 0} \mathbb{F}e_i \quad \text{y} \quad W_0^+ := \bigoplus_{i \geq 1} \mathbb{F}e_i.$$

El álgebra W_1 se conoce como *Álgebra de Witt*, es simple al igual que $\mathcal{V}ir$ y ambas satisfacen identidades polinómicas. Las álgebras W_0 y W_0^+ no son álgebras simples y requerirán un estudio un poco más detallado.

En el párrafo anterior hemos definido la noción de polinomio elíptico f sobre el álgebra $\mathcal{A}$. El polinomio f se dice que es elíptico sobre el álgebra $\mathcal{A}$ (o que tiene anchura finita sobre $\mathcal{A}$) si existe $m \geq 1$ tal que

$$Span_\Phi(f(\mathcal{A})) = \overbrace{f(\mathcal{A}) + ... + f(\mathcal{A})}^{m}.$$

Ahora definiremos una noción más fuerte.

Definición 5.3.1. *El polinomio f es fuertemente elíptico sobre $\mathcal{A}$ si existe un conjunto finito de $(n-1)$-tuplas, $M \subset \overbrace{\mathcal{A} \times ... \times \mathcal{A}}^{n-1}$ tal que*

$$f(\mathcal{A}) \subset \sum_{(a_1,...,a_{n-1})\in M} f(\mathcal{A}, a_1, ..., a_{n-1}).$$

Lema 5.3.1. *Un polinomio fuertemente elíptico sobre un álgebra $\mathcal{A}$ es también elíptico sobre $\mathcal{A}$.*

Demostración. Basta observar que en

$$Span_\Phi(f(\mathcal{A})) = \sum_{(a_1,...,a_{n-1})\in M} f(\mathcal{A}, a_1, ..., a_{n-1}),$$

el número de sumandos en la parte derecha es siempre menor o igual que $\mid M \mid$. □

Veremos que los polinomios multilineales son fuertemente elípticos tanto el álgebra de Virasoro como las subálgebras anteriormente definidas.

Teorema 5.3.2. *Un polinomio multilineal es fuertemente elíptico en $\mathcal{V}ir$ y en W_1.*

Demostración. Consideremos $\mathcal{L} = \mathcal{V}ir$ ó W_1 y $f(x_0, x_1, ..., x_{n-1})$ un elemento multilineal del álgebra de Lie libre. De este modo se tiene que

$$f = \sum_{\pi\in S_{n-1}} \alpha_\pi [x_0, x_{\pi(1)}, ..., x_{\pi(n-1)}], \quad \alpha_\pi \in \mathbb{F}.$$

Sea $M = \{(e_{i_1}, ..., e_{i_{n-1}}) \mid 0 \leq i_1 \leq ... \leq i_{n-1} \leq n\}$. Es claro que M es finito. Veamos que se cumple que

$$\mathcal{L} = \sum_{(e_{i_1},...,e_{i_{n-1}})\in M} f(\mathcal{L}, e_{i_1}, ..., e_{i_{n-1}}).$$

En efecto, elijamos $s \in \mathbb{Z}$. Entonces

$$f(e_{s-i_1-...-i_{n-1}}, e_{i_1}, ..., e_{i_{n-1}}) = h(s, i_1, ..., i_{n-1})e_s,$$

dónde

$h(s, i_1, ..., i_{n-1}) =$

$\sum \alpha_\pi (s - i_1 - ... - i_{n-1} - i_{\pi(1)})(s - i_1 - ... - i_{n-1} + i_{\pi(1)} - i_{\pi(2)})...$

$...(s - i_1 - ... - i_{n-1} + i_{\pi(1)} + ... + i_{\pi(n-2)} - i_{\pi(n-1)})$

es un polinomio homogéneo en $s, i_1, ..., i_{n-1}$ de grado n.

Si $f = 0$ es una identidad en $\mathcal{L}$, no hay nada que probar. En otro caso, $f(\mathcal{L}) \neq (0)$. Entonces $Span_{\mathbb{F}}(f(\mathcal{L}))$ es un ideal del álgebra $\mathcal{L}$ y puesto que $\mathcal{L}$ es simple, se sigue que $Span_{\mathbb{F}}(f(\mathcal{L})) = \mathcal{L}$.

Por tanto, para alguna elección de $i_1, ..., i_{n-1}$ tendremos que

$$f(e_{s-i_1-...-i_{n-1}}, e_{i_1}, ..., e_{i_{n-1}}) = e_s, \quad h(s, i_1, ..., i_{n-1}) = 1.$$

Si

$$e_s \notin \sum_{(e_{i_1},...,e_{i_{n-1}})\in M} f(e_{s-i_1-...-i_{n-1}}, e_{i_1}, ..., e_{i_{n-1}}),$$

entonces se tiene que $h(s, i_1, ..., i_{n-1}) = 0$ para todas las $(n-1)$-tuplas $(i_1, ..., i_{n-1}) \in [0, n]^{n-1}$.

Basta ahora usar que si un polinomio (no homogéneo) $g(x_1, ..., x_{n_1})$ de grado menor o igual que n se anula sobre $[0, n]^{n-1}$ entonces se tiene que $g = 0$. □

Para probar la elipticidad de polinomios multilineales en las álgebras W_0 y W_0^+ usaremos el hecho de que sus ideales tienen una forma muy precisa.

Lema 5.3.3. *Sea $\mathcal{L} = W_0$ o W_0^+. Tomemos un ideal $(0) \neq \mathcal{I}$ del álgebra $\mathcal{L}$. Entonces existe $i \in \mathbb{N}$ tal que*

$$\bigoplus_{j\geq i} \mathbb{F}e_j \subset \mathcal{I}$$

Demostración. Tomemos $0 \neq a \in \mathcal{I}$, se tiene que $a = \alpha_1 e_{i_1} + \alpha_2 e_{i_2} + ... + \alpha_m e_{i_m}$ para ciertos $i_1, ..., i_m \in \mathbb{N}$.

Conmutando por e_{i_1} tenemos que

$$[a, e_{i_1}] = (i_2 - i_1)\alpha_2 e_{i_1+i_2} + ... + (i_m - i_1)\alpha_m e_{i_1+i_m}.$$

Si ahora conmutamos por $e_{i_1+i_2}$ eliminaremos otro sumando en la expresión anterior y reiterando el proceso obtenemos que $\exists e_t \in \mathcal{I}$ para algún entero t suficientemente grande $(t \geq (m-1)i_1 + (m-2)i_2 + ... + i_m)$.

Este hecho nos lleva de manera inmediata a que todo elemento e_j, con $j \geq t$, pertenecerá también al ideal, por lo que

$$\bigoplus_{j\geq t} \mathbb{F}e_j \subset \mathcal{I}.$$

□

Es decir, cualquier ideal en W_0 o W_0^+ contiene todos los subespacios $\mathbb{F}e_i$, para i suficientemente grande, y por tanto tiene codimensión finita. En el caso de W_0, la presencia del elemento básico e_0 que juega un papel distinto al resto de elementos de la base, permite mejorar la descripción de los ideales.

Corolario 5.3.4. *Sea $\mathcal{L} = W_0$. Tomemos un ideal $(0) \neq \mathcal{I}$ del álgebra $\mathcal{L}$. Entonces existe $i \in \mathbb{N}$ tal que*

$$\mathcal{I} = \bigoplus_{j \geq i} \mathbb{F}e_j.$$

Demostración. Basta tomar un elemento no nulo a en el ideal $\mathcal{I}$, entonces $a = \alpha_1 e_{i_1} + \alpha_2 e_{i_2} + ... + \alpha_m e_{i_m}$ para ciertos $i_1, ..., i_m \in \mathbb{N}$. Aplicando un argumento similar al aplicado en el lema 5.3.3 tendremos que

$$b := [a, a_0] = (i_1\alpha_1 e_{i_1} + i_2\alpha_2 e_{i_2} + ... + i_m\alpha_m e_{i_m}).$$

Calculando $i_m a - b$ se elimina el sumando correspondiente al elemento básico e_{i_m}. Repitiendo este proceso $m-1$ veces se obtiene el resultado. □

Cabe destacar que W_0 contiene un único ideal maximal que es exactamente el álgebra de Witt positiva W_0^+. Esto no ocurre en W_0^+. Por ejemplo, si consideramos los ideales de W_0^+ generados por los elementos e_2 y $e_1 + e_2$ respectivamente, ambos son maximales y evidentemente distintos.

Probaremos ahora que un polinomio multilineal es fuertemente elíptico en W_0 y W_0^+. Usaremos que todo ideal en cualquiera de las dos álgebras tiene codimensión finita.

Teorema 5.3.5. *Un polinomio multilineal es fuertemente elíptico en W_0 y W_0^+.*

Demostración. La demostración sigue las mismas lineas del teorema 5.3.2. Consideremos $\mathcal{L} = W_0$ ó W_0^+ y $f(x_0, x_1, ..., x_{n-1})$ un elemento multilineal del álgebra de Lie libre y supongamos que f no es una identidad en $\mathcal{L}$. Se tiene que

$$f = \sum_{\pi \in S_{n-1}} \alpha_\pi [x_0, x_{\pi(1)}, ..., x_{\pi(n-1)}], \quad \alpha_\pi \in \mathbb{F}.$$

Consideremos el conjunto $M_1 = \{(e_{i_1}, ..., e_{i_{n-1}}) \mid 1 \leq i_1 \leq ... \leq i_{n-1} \leq n\}$ que es claramente finito.

Para cualquier $s \in \mathbb{Z}$ tal que $s > i_1 + ... + i_{n-1}$ tendremos que

$$f(e_{s-i_1-...-i_{n-1}}, e_{i_1}, ..., e_{i_{n-1}}) = h(s, i_1, ..., i_{n-1})e_s,$$

dónde

$$h(s, i_1, ..., i_{n-1}) =$$

$$\sum \alpha_\pi (s - i_1 - ... - i_{n-1} - i_{\pi(1)})(s - i_1 - ... - i_{n-1} + i_{\pi(1)} - i_{\pi(2)})...$$

$$...(s - i_1 - ... - i_{n-1} + i_{\pi(1)} + ... + i_{\pi(n-2)} - i_{\pi(n-1)})$$

es un polinomio homogéneo en $s, i_1, ..., i_{n-1}$ de grado n.

Sabemos que $Span_{\mathbb{F}}(f(\mathcal{L}))$ es un ideal del álgebra $\mathcal{L}$, por lo que aplicando el lema 5.3.3 tendremos que existe un $k \in \mathbb{N}$ tal que $e_t \in Span_{\mathbb{F}}(f(\mathcal{L}))$ para todo $t \geq k$.

Es decir, existe un $k \in \mathbb{N}$ tal que para todo $s \geq k$ se tiene que $e_s \in Span_{\mathbb{F}}(f(\mathcal{L}))$

Por tanto, $\exists i_1, ..., i_{n-1}$ tales que $s > i_1 + ... + i_{n-1}$ y $h(s, i_1, ..., i_{n-1}) = 1$. Como en el teorema 5.3.2 tendremos que

$$e_s \in \sum_{(e_{i-1}, ..., e_{i_{n-1}}) \in M_1} f(\mathcal{L}, e_{i_1}, ..., e_{i_{n-1}}).$$

Como la codimensión en $\mathcal{L}$ de $\mathbb{F}(e_s, e_{s+1}, ...)$, $\mid \mathcal{L} : \mathbb{F}(e_s, e_{s+1}, ...) \mid$, es finita, se tiene que

$$\mid Span_{\mathbb{F}}(f(\mathcal{L})) : \mathbb{F}(e_s, e_{s+1}, ...) \mid = r,$$

es finita.

Tomando un subespacio de $Span_{\mathbb{F}}(f(\mathcal{L}))$ complementario de $\mathbb{F}(e_s, e_{s+1}, ...)$, sea $\mathbb{F}(e_1, ..., e_r)$, podemos expresar cada e_j como

$$e_j = \sum_{finita} f(a_0^j, e_{j_1}^j, ..., e_{j_{n-1}}^j), \quad j = 1, ..., r.$$

Es decir,

$$e_1, ..., e_r \in \sum_{(e_{j_1}, ..., e_{j_{n-1}}) \in M_2} f(\mathcal{L}, e_{j_1}, ..., e_{j_{n-1}}),$$

siendo $M_2 = \{(e_{j_1}^j, ..., e_{j_{n-1}}^j) \mid j = 1, ..., r\}$ el conjunto de las tuplas que aparecen involucradas en la expresión de $e_1, ..., e_r$.

Basta tomar $M = M_1 \cup M_2$ para tener que

$$Span_{\mathbb{F}}(f(\mathcal{L})) = \sum_{(e_{i-1}, ..., e_{i_{n-1}}) \in M} f(\mathcal{L}, e_{i_1}, ..., e_{i_{n-1}}).$$

□

5.4. Grupo de Nottingham en característica 0

Dado un cuerpo $\mathbb{F}$ de característica prima p, el Grupo de Nottingham sobre $\mathbb{F}$ puede verse como el grupo de automorfismos normalizados del cuerpo $\mathbb{F}((t))$. Podemos considerar el grupo de Nottingham como el conjunto

$$N_{\mathbb{F}}(t) := \{t + \sum_{k\geq 1} \alpha_k t^{k+1} \mid \alpha_k \in \mathbb{F} \quad \forall k \in \mathbb{N}\},$$

en el que dados dos elementos f, g en $N_{\mathbb{F}}(t)$, con $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ y $g = t + \sum_{k\geq 1} \beta_k t^{k+1}$ definimos la siguiente operación:

$$fg := g(f) = f + \sum_{k\geq 1} \beta_k f^{k+1}.$$

Es un pro-p grupo finitamente generado con propiedades que han sido ampliamente estudiadas en la teoría de pro-p grupos.

Nosotros consideraremos el grupo de Nottingham en característica 0, que comparte una serie de propiedades con el grupo de Nottingham en característica prima. En lo que sigue, $\mathbb{F}$ será un cuerpo (no necesariamente de característica prima) y $N_{\mathbb{F}}(t)$ el grupo de Nottingham sobre $\mathbb{F}$.

Definición 5.4.1. *Dado un elemento $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ del grupo de Nottingham $N_{\mathbb{F}}(t)$, se define la profundidad de f como*

$$\delta(f) := inf\{k \in \mathbb{N} \mid \alpha_k \neq 0\} \in \mathbb{N} \cup \{\infty\}.$$

Denotemos para cada $i \geq 1$ por K_i al conjunto $\{f \in N_{\mathbb{F}}(t) \mid \delta(f) \geq i\}$. Cada K_i es un subgrupo normal de $N_{\mathbb{F}}(t)$. Podemos considerar para cada $n \in \mathbb{N}$ la siguiente relación en el grupo de Nottingham:

$$f \sim_n g \longleftrightarrow f - g + t \in K_n,$$

es decir, si $f - g = t^{n+1}h$ para algún $h \in N_{\mathbb{F}}(t)$.

Se tiene que

1. Para todo $n \in \mathbb{N}$, la relación $\sim_n$ es de equivalencia en $N_{\mathbb{F}}(t)$.

2. Para todo $n \in \mathbb{N}$, la relación $\sim_n$ conserva la composición en $N_{\mathbb{F}}(t)$, es decir, si $f \sim_n g$ y $f' \sim_n g'$ entonces $ff' \sim_n gg'$.

Podemos considerar para cada $i \in \mathbb{N}$ el conjunto $N_i := N_{\mathbb{F}}(t)/\sim_i$. La composición de polinomios en $N_{\mathbb{F}}(t)$ induce una operación binaria en cada N_i y podemos construir de manera natural los homomorfismos:

$$\tau_n : N_{\mathbb{F}}(t) \longrightarrow N_n, \quad \sigma_n : N_{n+1} \longrightarrow N_n$$

tales que $\tau_{n+1}\sigma_n = \tau_n$ para todo $n \in \mathbb{N}$.

En [9] se da la construcción del Grupo de Nottingham como límite inverso de un sistema inverso de grupos

Lema 5.4.1. *1. Para cada $n \in \mathbb{N}$, N_n es un grupo finito.*

2. $N_{\mathbb{F}}(t)$ es el límite inverso del sistema $\{(N_i, \sigma_i) \mid i \in \mathbb{N}\}$.

3. $N_{\mathbb{F}}(t)$ es un grupo profinito.

Lema 5.4.2. *Para todo $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ en el grupo de Nottingham $N_{\mathbb{F}}(t)$ se tiene que $\delta(f) = \delta(f^{-1})$.*

Demostración. Supongamos que $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ y que $f^{-1} = t + \sum_{k\geq 1} \beta_k t^{k+1}$. Entonces

$$\begin{array}{rcccccl} ff^{-1} & = & f^{-1}(f) & = & f + \sum_{k\geq 1} \beta_k f^{k+1} & = & t \\ f^{-1}f & = & f(f^{-1}) & = & f^{-1} + \sum_{k\geq 1} \alpha_k (f^{-1})^{k+1} & = & t, \end{array}$$

de donde se obtiene que

$$\begin{array}{rcl} f & = & t + \sum_{k\geq 1}(-\beta_k) f^{k+1} \\ f^{-1} & = & t + \sum_{k\geq 1}(-\alpha_k)(f^{-1})^{k+1}, \end{array}$$

y por tanto $\delta(f) = \delta(f^{-1})$. □

Definición 5.4.2. *Dado un elemento $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ del grupo de Nottingham $N_{\mathbb{F}}(t)$ tal que $\delta(f) = k \in \mathbb{N}$, definimos el primer coeficiente de f como*

$$\rho(f) := \alpha_k.$$

Lema 5.4.3. *Si tomamos f, g elementos en el grupo de Nottingham $N_{\mathbb{F}}(t)$ distintos de la identidad se verifica*

1. *Si $\delta(f) = \delta(g)$ entonces $\rho(fg) = \rho(f) + \rho(g) = \rho(gf)$. Por tanto, $\rho(f^{-1}) = -\rho(f)$.*
2. *$\rho(f^n) = n\rho(f)$ para todo $n \in \mathbb{N}$.*

Demostración. Es evidente que basta probar 1. Consideremos entonces $f = t + \sum_{k\geq 1} \alpha_k t^{k+1}$ y $g = t + \sum_{k\geq 1} \beta_k t^{k+1}$ de manera que $\delta(f) = \delta(g)$.

$$gf = f(g) = g + \sum_{k\geq 1} \alpha_k g^{k+1},$$

Si $\rho(g) = \beta_n$ y $\rho(f) = \alpha_n$, se tiene que para todo $k < n$ el coeficiente de t^k en gf es 0.

Para $k = n$, el coeficiente de t^n en gf es $\beta_n + \alpha_n$.

De este modo $\rho(gf) = \beta_n + \alpha_n = \rho(f) + \rho(g)$. □

El siguiente resultado proporciona, de manera explícita, el primer coeficiente del conmutador de dos elementos en el grupo de Nottingham $N_{\mathbb{F}}(t)$. Para más detalles puede consultarse [9].

Lema 5.4.4. *Sean* $\alpha = t + \alpha_{m-1}t^m + \sum_{k\geq m} \alpha_k t^{k+1}$ *y* $\beta = t + \beta_{n-1}t^n + \sum_{k\geq n} \alpha_k t^{k+1}$ *dos elementos en el grupo de Nottingham* $N_{\mathbb{F}}(t)$*, con* $\rho(\alpha) = \alpha_{m-1}$ *y* $\rho(\beta) = \beta_{n-1}$*. Se tiene que*

$$[\alpha, \beta] = t + \alpha_{m-1}\beta_{n-1}(m-n)t^{m+n-1} + f(t),$$

con el grado de $f(t)$ *mayor o igual a* $m + n$*. Es decir,*

$$\rho([\alpha, \beta]) = \rho(\alpha)\rho(\beta)(\delta(\alpha) - \delta(\beta)).$$

A partir de ahora, consideraremos que la característica de $\mathbb{F}$ es 0.

Lema 5.4.5. *El Grupo de Nottingham sobre un cuerpo de característica* 0 *es libre de torsión.*

Demostración. Basta tener en cuenta que $\rho(f) = 0$ si y sólo si $f = t$, que $\rho(f^n) = n\rho(f)$ y aplicar el lema 5.4.3. □

Consideremos los conjuntos $K_i := \{f \in N_{\mathbb{F}}(t) \mid \delta(f) \geq i\}$. Se verifica:

1. Para todo $i \in \mathbb{N}$ se tiene que $K_i \trianglelefteq N_{\mathbb{F}}(t)$ y que $K_{i+1} \trianglelefteq K_i$.
2. Como consecuencia del lema 5.4.4 se tiene que, $[K_i, K_j] \subset K_{i+j}$ para todo $i, j \in \mathbb{N}$.
3. Se tiene que $K_i/K_{i+1} \simeq \mathbb{F}$.

Para ver el último punto basta darse cuenta que si $a, b \in K_i \setminus K_{i+1}$ se tiene que $\delta(a) = \delta(b) = i$ y podemos aplicar entonces el lema 5.4.3. De este modo tendremos que

$$ab^{-1} \in K_{i+1} \Leftrightarrow \delta(ab^{-1}) \leq i + 1 \Leftrightarrow$$

$$\Leftrightarrow \rho(a) + \rho(b^{-1}) = \rho(a) - \rho(b) = 0 \Leftrightarrow \rho(a) = \rho(b),$$

de donde se obtiene que las clases aK_{i+1} y bK_{i+1} son iguales.

Nota: La aplicación

$$\begin{aligned} \theta : K_i/K_{i+1} &\longrightarrow \mathbb{F} \\ aK_{i+1} &\mapsto \rho(a) \end{aligned}$$

es una biyección y verifica que

$$\theta(abK_{i+1}) = \theta(aK_{i+1}) + \theta(bK_{i+1}),$$

para todo $aK_{i+1}, bK_{i+1} \in K_i/K_{i+1}$.

A través de θ, K_i/K_{i+1} tiene estructura de $\mathbb{F}$-espacio vectorial definiendo

$$aK_{i+1} + bK_{i+1} = abK_{i+1} \quad \text{para todo} \quad aK_{i+1}, bK_{i+1} \in K_i/K_{i+1},$$

$$\lambda(aK_{i+1}) = (t + \lambda a_i t^{i+1} + ...)K_{i+1},$$

para todo $\lambda \in \mathbb{F}$ y todo $aK_{i+1} = (t + a_i t^{i+1} + ...)K_{i+1} \in K_i/K_{i+1}$.

De este modo tendremos que fijado el grupo $N_{\mathbb{F}}(t)$, la serie de subgrupos normales $(K_i)_{i\geq 1}$ es una filtración del grupo de Nottingham. Podemos construir un álgebra de Lie asociada a la filtración (K_i) del grupo de Nottingham $N_{\mathbb{F}}(t)$.

$$\mathcal{L}(N_{\mathbb{F}}(t), (K_i)) := \bigoplus_{i\geq 1} K_i/K_{i+1},$$

que es un álgebra de Lie sobre $\mathbb{F}$ cuyo corchete de Lie viene dado por la expresión

$$[aK_{i+1}, bK_{j+1}] = (a, b)K_{i+j+1},$$

siendo (a, b) el conmutador de los elementos a y b en el grupo de Nottingham $N_{\mathbb{F}}(t)$.

Dados los elementos $f = t + \sum_{i\geq m} \alpha_i t^{i+1}$ y $g = t + \sum_{j\geq n} \alpha_j t^{j+1}$ del grupo de Nottingham, la igualdad del lema 5.4.4 origina

$$(f, g) = t + (m - n)\alpha_m\beta_n t^{n+m+1} \quad mod(K_{n+m+1}),$$

de donde se obtiene fácilmente la expresión para el corchete de Lie:

$$[aK_{n+1}, bK_{m+1}] = t + (m - n)\alpha_m\beta_n t^{n+m+1} K_{n+m+1}.$$

Recordemos la construcción del álgebra de Witt positiva sobre $\mathbb{F}$, W_0^+, se tiene

- W_0^+ tiene una base $\{e_n \mid n \geq 1\}$ cuyo corchete de Lie viene definido por $[e_n, e_m] = (m - n)e_{n+m}$ para todos $n, m \geq 1$.

Como se puede observar hay cierta similitud entre el álgebra de Lie asociada al grupo de Nottingham $N_{\mathbb{F}}(t)$ a través de la filtración (K_i), $\mathcal{L}(N_{\mathbb{F}}(t),(K_i))$ y el álgebra de Witt positiva, W_0^+.

De este modo podemos construir el siguiente isomorfismo de álgebras de Lie

$$\mathcal{L}(N_{\mathbb{F}}(t),(K_i)) \simeq \bigoplus_{i\geq 1} \mathbb{F}x_i,$$

dónde $x_i = (t+t^{i+1})K_{i+1}$ y $\lambda x_i = (t+\lambda t^{i+1})K_{i+1}$.

Se tiene que

$$[x_i,x_j] = [(t+t^{i+1})K_{i+1},(t+t^{j+1})K_{j+1}] = (t+(i-j)t^{i+j+1})K_{i+j+1} = (i-j)x_{i+j+1},$$

por lo que

$$W_0^+ \simeq \mathcal{L}(N_{\mathbb{F}}(t),(K_i)).$$

Llegados a este punto podemos enunciar el siguiente resultado.

Corolario 5.4.6. *Todo polinomio multilineal es fuertemente elíptico sobre el álgebra de Lie ligada a la filtración generada por la familia de subgrupos $(K_i)_{i\geq 1}$ del Grupo de Nottingham $N_{\mathbb{F}}(t)$.*

Demostración. Basta observar que

$$W_0^+ \simeq \mathcal{L}(N_{\mathbb{F}}(t),(K_i))$$

y aplicar el lema 5.3.5 para obtener el resultado. □

Es usual considerar el álgebra de Lie asociada a un grupo a través de su serie central descendente. En el caso del grupo de Nottingham no coincide exactamente con la asociada a la filtración (K_i), pero está muy cerca.

En lo que sigue $\gamma_n(G)$ hará referencia al término n-ésimo de la serie central descendente de un grupo G, es decir, $\gamma_1(G) = G$ y $\gamma_n(G) = [\gamma_{n-1}(G),G]$ para todo $n > 1$.

Lema 5.4.7. *([9]) Dado el grupo de Nottingham $N_{\mathbb{F}}(t)$ se tiene que para todo $n \geq 2$, $\gamma_n(N_{\mathbb{F}}(t)) = K_{n+1}$.*

Visto el anterior resultado, podemos construir el álgebra de Lie ligada a la filtración de la serie central descendente del grupo de Nottingham $N_{\mathbb{F}}(t)$.

$$\mathcal{L}(N_{\mathbb{F}}(t),(\gamma_n(N_{\mathbb{F}}(t)))_{n\geq 1}) = (N_{\mathbb{F}}(t)/K_3) \oplus (\bigoplus_{i\geq 3} K_i/K_{i+1}).$$

Ambas álgebras graduadas coinciden en los términos finales

$$\bigoplus_{i\geq 3} K_i/K_{i+1}.$$

La diferencia entre ambas estructuras radica en que el primer término del álgebra de Lie asociada a la serie central descendente $\mathcal{L}(N_{\mathbb{F}}(t)$ es un álgebra de Lie abeliana de dimensión 2, mientras que los dos primeros términos del álgebra de Witt positiva W_0^+ son 1-dimensionales.

Este detalle nos confirma definitivamente que dichas álgebras no pueden ser isomorfas, pues en el álgebra de Witt positiva W_0^+ no existen dos elementos linealmente independientes cuyo corchete de Lie sea 0.

Sin embargo encontramos un ideal $\mathcal{I}$, que es común en ambas álgebras y cuya codimensión en cada una de ellas es 1. Dicho ideal es

$$\bigoplus_{i\geq 2} K_i/K_{i+1}.$$

Los lemas 5.3.3 y 5.3.5 en los que se construyen los ideales de las álgebras W_0 y W_0^+ y se prueba que todo polinomio multilineal es fuertemente elíptico sobre ambas álgebras son válidos en el álgebra $\mathcal{L}(N_{\mathbb{F}}(t), (\gamma_n(N_{\mathbb{F}}(t)))_{n\geq 1})$, por lo que podemos enunciar el siguiente resultado.

Teorema 5.4.8. *Todo polinomio multilineal es fuertemente elíptico sobre el álgebra de Lie ligada a la filtración de la serie central descendente del Grupo de Nottingham* $N_{\mathbb{F}}(t)$.

No existen resultados que relacionen el hecho de que toda palabra del grupo libre sea elíptica en un grupo G con que todo polinomio multilineal sea fuertemente elíptico en el álgebra de Lie asociada a su serie central descendente. Por ello trataremos de probar que todo palabra del grupo libre $\mathcal{F}_r$ es elíptica sobre el grupo $N_{\mathbb{F}}(t)$ directamente.

Definición 5.4.3. *Dada una clase de grupos* $\mathcal{C}$*, decimos que un grupo* G *es justo un no-*$\mathcal{C}$*-grupo (just non* $\mathcal{C}$*-group) si* $G \notin \mathcal{C}$ *pero todo cociente propio de* G *está en* $\mathcal{C}$.

Así, un grupo G *se dice justo no nilpotente (just non-nilpotent) si todo cociente propio es nilpotente, pero* G *no es nilpotente.*

Teorema 5.4.9. *Sea* G *un grupo finitamente generado (como grupo topológico), pronilpotente y justo no nilpotente. Entonces, o bien* G *es resoluble o cualquier palabra arbitraria* ω *del grupo libre* $\mathcal{F}$ *es elíptica en* G.

Demostración. Podemos suponer $\omega(G) \neq 1$ y sea $H = \langle \omega(G) \rangle$. Entonces, el grupo cociente G/H es nilpotente.

Si el grupo H es abeliano, entonces G es un grupo resoluble. Supongamos entonces que $[H,H] \neq 1$. En ese caso, el grupo factor $G/\overline{[H,H]}$ será un grupo nilpotente y finitamente generado.

El grupo H está (topológicamente) generado por los generadores de H módulo $\overline{[H,H]}$. Como todo subgrupo de un grupo nilpotente y finitamente generado es finitamente generado, podemos concluir que existen elementos $h_1, ..., h_r \in \omega(G)$ que generan el grupo H.

De este modo tendremos que

$$[H,H] = [H,h_1][H,h_2]...[H,h_r]$$

es un subconjunto cerrado de G.

Es sabido (Romankov lo demostró para grupos policíclicos en [25]) que toda palabra ω es elíptica sobre un grupo nilpotente y finitamente generado. De este modo tendremos que existe un natural $N > 1$ tal que

$$\omega(G) \subset \overbrace{\omega(G)^{\pm 1}...\omega(G)^{\pm 1}}^{N}\overline{[H,H]} = \overbrace{\omega(G)^{\pm 1}...\omega(G)^{\pm 1}}^{N}[H,h_1][H,h_2]...[H,h_r].$$

De este modo, la anchura verbal de la palabra ω en G será siempre menor o igual que $N + 2r$. □

Para poder aplicar el resultado anterior al grupo de Nottingham son necesarios los siguientes resultados.

Lema 5.4.10. *Sea G un grupo pronilpotente. Consideremos la serie central descendente $G = G_1 > G_2 > ...$ y $\mathcal{L} = \oplus_{i \geq 1} L_i$, con $L_i := G_i/G_{i+1}$, el correspondiente anillo de Lie. Supongamos que $\mathcal{L}$ es graduada justo no nilpotente, es decir, que todo ideal graduado no nulo de $\mathcal{L}$ contiene $\oplus_{k \geq n} L_n$ para algún natural n. Entonces G es justo no nilpotente.*

Demostración. Sea $(1) \neq H$ un subgrupo normal cerrado de G. Tomemos $i \in \mathbb{N}$ el menor natural tal que $H \subset G_i$ (notar que $H \subset G_1$) y consideremos el subconjunto de L_i

$$V := \{hG_{i+1} \mid h \in H\},$$

que claramente contiene elementos distintos de 0.

Se tiene entonces que existe un natural $n \geq 1$ tal que

$$L_n \subset \sum [V, \overbrace{L_1, ..., L_1}^{n-i}].$$

Esto nos lleva a que un elemento arbitrario de G_n es igual, módulo G_{n+1}, a un producto de conmutadores de la forma $[h, g_1, ..., g_{n-i}]$, dónde $h \in H$ y $g_1, ..., g_{n-i} \in G$.

Argumentando de este mismo modo con $G_{n+1}, G_{n+2}, ...$ podemos concluir que G_n está en el subgrupo cerrado H. Esto prueba que G/H es nilpotente, con lo que el lema queda demostrado. □

Consideremos ahora un cuerpo $\mathbb{F}$ y tomemos el álgebra de Virasoro sin centro $\mathcal{V}ir := \oplus_{n\mathbb{Z}}\mathbb{F}e_n$. Consideremos $d \geq 1$ y tomemos $\mathcal{L}_d = \oplus_{i\geq d}\mathbb{F}e_i = \mathcal{L}$.

Lema 5.4.11. *El álgebra de Lie $\mathcal{L}$ es graduada y justo no nilpotente.*

Demostración. Tomemos un ideal graduado $(0) \neq \mathcal{I} \trianglelefteq \mathcal{L}$ y sea $0 \neq a_k \in \mathcal{I} \cap L_k$. Entonces, para un natural arbitrario $i \geq max(2k+1, k+d)$ tendremos que

$$L_i = [a_k, L_{i-k}] \subset \mathcal{I},$$

lo que nos demuestra el resultado. □

Una vez probados estos dos resultados, podemos volver al grupo de Nottingham $N_{\mathbb{F}}(t)$. Tendremos, en virtud del lema 5.4.11 que el álgebra de Lie $\mathcal{L}(N_{\mathbb{F}}(t), (\gamma_n(N_{\mathbb{F}}(t)))_{n\geq 1})$ es graduada y justo no nilpotente. Debido a que $N_{\mathbb{F}}(t)$ es un grupo pronilpotente, una aplicación directa del lema 5.4.10 nos lleva a concluir que $N_{\mathbb{F}}(t)$ es justo no nilpotente. Podemos ya enunciar el resultado principal de esta sección.

Teorema 5.4.12. *Toda palabra ω del grupo libre $\mathcal{F}$ es elíptica sobre el grupo de Nottingham en característica* 0*, $N_{\mathbb{F}}(t)$.*

Demostración. En vista de que el grupo $N_{\mathbb{F}}(t)$ no es resoluble, basta con una aplicación directa del teorema 5.4.9 para obtener el resultado. □

Conclusiones y trabajo futuro

El objetivo de esta tesis ha sido el estudio de subgrupos verbales y anchuras verbales en grupos. El propósito central era estudiar palabras de Engel en grupos alternados y el fin último era conseguir demostrar que todo elemento en un grupo alternado A_n, $n \geq 5$, se puede escribir como una palabra de Engel de longitud arbitraria. Este objetivo final no se ha culminado, siendo uno de los objetivos para el trabajo futuro. Pero se han conseguido avances significativos.

En el primer capítulo se considera la palabra x^{p^k} y se prueba que su anchura verbal en los grupos alternados A_n, $n \geq 5$, es a lo sumo 2. Es decir, que todo elemento de A_n se puede expresar como producto de dos potencias p^k-ésimas de elementos de A_n. Aunque este resultado se sigue de otros profundos resultados de Guralnik (ver [6]), hemos querido incluirlo por la simplicidad de las técnicas empleadas, que no requieren conocer las potentes herramientas usadas por Guralnik en su trabajo.

En el capítulo 2 probamos que todo elemento de A_n se puede expresar como producto de dos palabras de Engel de longitud arbitraria. Aunque Shalev et al. ([19]) habían considerado este problema y probado el resultado para grupos simples suficientemente grandes, el resultado del capítulo 2 no es consecuencia del mismo, ya que es válido para todo A_n, $n \geq 5$.

En el capítulo 3 se da respuesta al objetivo central de la tesis para palabras de Engel de longitud 2.

Con el fin de aproximarnos al objetivo en su versión general, que parece inabordable, exploramos una aproximación combinatoria que permitió resultados computacionales para ciertos valores de n. Los resultados, explicados en el capítulo 4 de la tesis, permiten confirmar la conjetura para valores que antes habían sido intratables y para todo m.

Por tanto, el problema de si se puede expresar todo elemento de A_n como una palabra de Engel de longitud arbitraria tiene respuesta afirmativa para $5 \leq n \leq 14$.

Creemos que esta vía puede ser explotada para ayudar a demostrar el problema originario de la tesis, un problema de gran dificultad en el que han trabajado expertos internacionales y al que, creemos, se dan avances interesantes en esta tesis.

El capítulo 5 es algo diferente a los anteriores. Se considera el grupo de Nottingham, ejemplo importante de grupo profinito. Este grupo ha sido muy estudiado, especialmente en el caso de característica prima. En este caso, Klopsch ([12]) demostró que toda palabra tiene anchura finita.

Nuestro objetivo ha sido demostrar el mismo resultado en caso de característica 0. Para ello se ha considerado el álgebra de Lie asociada a través de su serie central descendente y se ha estudiado el problema análogo en álgebras.

Finalmente, los resultados demostrados para el grupo de Nottingham en característica 0 y su álgebra de Lie asociada han sido independientes y, hasta donde sabemos, no hay resultados en esta linea que relacionen la situación en grupos y la correspondiente a su álgebra de Lie asociada.

Creemos que esta es una linea de trabajo interesante que merece ser explorada y que está entre nuestros objetivos de trabajo futuro.

Conclussions and future work

The aim of this thesis has been the study of verbal subgroups and verbal width in groups. The main purpose was to study Engel words in Alternating groups and our goal was to try to prove that every element in an Alternating group A_n, $n \geq 5$, can be written as an Engel word of arbitrary length. This goal has not been totally achieved and this is one of our aims for the future work. Nevertheless, significant progress has been achieved.

In the first Chapter we consider the word x^{p^k} and prove that its verbal width in the Alternating groups A_n, $n \geq 5$, is at most 2. That is, every element in an Alternating group A_n can be written as a product of two p^k-th powers of elements in A_n. Although this result can be deduced from other deep results by Guralnik (see [6]), we wanted to include it in this work because of the simplicity of the technics used that do not require the knowledge of the powerful tools used by Guralnik in his work.

In Chapter 2 we proved that every element in an Alternating group A_n can be written as a product of two Engel words of arbitrary length. Although Shalev et al. ([19]) had considered and proved this problem for simple groups big enough, the result of Chapter 2 is not a consequence of their result, since we have proved it for every Alternating group A_n, $n \geq 5$.

In Chapter 3 we give an answer to the central aim of this thesis for Engel words of length 2.

In order to give an approach to the general case of this problem, which seems to be unapproachable, we studied a combinatorial approach that allowed us to find computational results for some values of n. These results, explained in Chapter 4, confirm the conjecture for some values of n, that could not be treated before, and for every m.

So now, we can say that an arbitrary element of A_n, $5 \leq n \leq 14$, can be written as an Engel word of arbitrary length.

We hope that this method can be helpful to prove the initial problem of this thesis, a problem of high difficulty in which international experts have

been working and for which, in our opinion, we have given some interesting advances in this thesis.

Chapter 5 is somehow different from the previous ones. In it, we consider the Nottingham group, an interesting example of profinite group. This group has been widely studied, especially in case of prime characteristic. In this case, Klopsch ([12]) proved that every word has finite width.

Our aim has been to prove the same result for the Nottingham group in zero characteristic. For that, we have considered the Lie algebra associated to the lower central series of the Nottingham group and we have studied the analogous problem in algebras.

Finally, the results proved for the Nottingham group in zero characteristic and in its associated Lie algebra have been independent. And, as far as we know, there are not results that establish a relation between the fact that every word is elliptic in a group and the corresponding situation in its associated Lie algebra.

We believe that this is an interesting line of research that deserves to be explored and that is also between our future research plans.

Bibliografía

[1] E. Bertram, *Even Permutations as a Product of Two Conjugate Cycles.* Journal of Combinatorial Theory 12 (1972), pp. 368-380.

[2] E. Bertram, *Powers of Cycle-Classes in Symmetric Groups.* Journal of Combinatorial Theory 94 (1999), pp 87-99.

[3] E. W. Ellers and N. L. Gordeev, *On the conjectures of J. Thompson and O. Ore.* Trans. Amer. Math. Soc. 350, no. 9 (1998), 3657-3671

[4] W.J. Ellision, *Warings's Problem* (Survey). American Mathematical Monthly, volume 78 (1971), pp. 10-36.

[5] F.G. Frobenius,Über Gruppencharacktere, Sitzber. Preuss. Akad. Wis. (1896) pp. 985-1021.

[6] R. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces.* J. Amer. Math. Soc. 25 (2012), no. 1, 77-121

[7] B. Harltey, *Subgroups of finite index in profinite groups.* Math. Zeit. 168 (1979), pp. 71-76.

[8] G. James and M. Liebeck, *Representations and Characters of Groups.* Cambridge University Press (1993).

[9] D.L. Johnson, *The Group of Formal Power Series under Substitution.* J. Austral Math. Soc. (Series A) 45 (1988) pp. 296-302.

[10] Victor G. Kac, *Infinite dimensional Lie algebras.* Cambridge University Press (1990).

[11] F. Kasch, *Modules and Rings.* London Mathematical Society. Monograph n.17 (1982).

[12] B. Klopsch, *Normal Subgroups in Substitution Groups of Formal Power Series*, Journal of Algebra 228 (2000), pp. 91-106.

[13] B. Klopsch, *Automorphisms of the Nottingham Group*, Journal of Algebra 223 (1999), pp. 37-56.

[14] A. I. Kostrikin, *Around Burnside*. Ergebnisse der Mathematic and ihrer Grenzgebiete 3. Folge. A Series of Modern Surveys in Mathematics. Springer-Verlag. (1990)

[15] M. Larsen and A. Shalev, *World maps and Waring type problems*. Journal of the Ame. Math. Soc. 22 (2008) pp. 437-466.

[16] M.W. Liebeck, E.A. O'Brien,A. Shalev and P.H. Tiep. *The Ore Conjecture*. J. Eur. Math. Soc. 12 (2010) pp. 939-1008

[17] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep. *Products of squares in finite simple groups*. Amer. Math. Soc. 140 (2012), no. 1, pp. 21-33

[18] M.W. Liebeck and A. Shalev, *Diameter of simple groups: sharp rounds and applications*, Annals of Math. 154 (2001), pp. 383-406.

[19] M. J. Larsen, A. Shalev and P. H. Tiep, *The Waring problem for finite simple groups*. Ann. of Math. (2) 174 (2011), no. 3, pp. 1885-1950.

[20] J. Martínez Carracedo. Powers in Alternating Simple Groups. Extracta Mathematicae Vol. 30, Num. 2 (2015), pp. 251-262.

[21] J. Martínez Carracedo. Engel Words in Alternating Groups. Journal of Algebra and Its Applications. To appear (2016).

[22] C. Martinez and E. I. Zelmanov, *Product of powers in finite simple groups*. Israel J. Math. 96 (1996), pp. 469-479.

[23] O. Ore, *Some Remarks on Commutators*. Proc. Amer. Math. Soc. 2 (1951), pp.307-314.

[24] A. H. Rhemtulla, *A problem of bounded expressibility in free products*, Academic Press, New York, (1994).

[25] V.A. Romankov, *Width of verbal subgroups in solvable groups*, Algebra i logika 21 (1982), pp. 60-72.

[26] J. S. Rose, *A Course on Group Theory. Dover Publications*, INC. New York (1994).

[27] J. Saxl and J. S. Wilson, *A note on powers in simple groups*, Math. Proc. Camb. Phil. Soc. 122 (1997), pp. 91-94.

[28] W. R. Scott, *Group Theory. Dover Publications*. New York (1987).

[29] D. Segal, *Words: Notes on Verbal Width in Groups*. London Mathematical Society Lecture Notes Series 361 (2009).

[30] P. Stroud, *Topics in the theory of verbal subgroups*. PhD Thesis. University of Cambridge (1966).

[31] R. D. Wade, *The Lower Central Series of a Right-Angled Artin Group*, ArXiv: 1109.1722v1

[32] J. S. Wilson, *First-order group theory*. Infinite Groups 1996. Gruyter, Berlin (1996). pp. 301-314.

[33] K. A. Zhelakov, A. M. Slin'ko, I. P. Shestakov and A. I. Shirshov, *Rings that are nearly associative*. Academic Press, INC. (1982).

[34] *GAP Bibliography*: http://www.gap-system.org

Apéndice A

Publicaciones derivadas de la tesis

Título: Powers in Alternating Simple Groups.
Autor: Jorge Martínez Carracedo.
Revista de publicación: Extracta Mathematicae Vol. 30, Num. 2 (2015).

Powers in Alternating Simple Groups

Jorge Martínez Carracedo
Departamento de Matemáticas. Universidad de Oviedo.
C/ Calvo Sotelo, s/n, 33007 Oviedo.
Spain.

martinezjorge@uniovi.es

Abstract

C. Martínez and E. Zelmanov proved in [12] that for every natural number d and every finite simple group G, there exists a function $N = N(d)$ such that either $G^d = 1$ or $G = \{a_1^d ... a_N^d \mid a_i \in G\}$. In a more general context the problem of finding words ω such that the word map $(g_1, ..., g_d) \longrightarrow \omega(g_1, ..., g_d)$ is surjective for any finite non abelian simple group is a major challenge in Group Theory. In [8] authors give the first example of a word map which is surjective on all finite non-abelian simple groups, the commutator $[x, y]$ (Ore Conjecture). In [11] the conjecture that this is also the case for the word x^2y^2 is formulated. This conjecture was solved in [9] and, independently, in [6], using deep results of algebraic simple groups and representation theory. An elementary proof of this result for alternating simple groups is presented here.

Key Words: Alternating groups. Simple Groups. Power subgroups. Word maps.
2000 Mathematics Subject Classification: 20D06, 20B35.

1 Introduction

In any group G, G^d the subgroup generated by d-th powers of elements in G and G' are normal subgroups. So, if G is a finite non-abelian simple group it is clear that $G = G'$ and if d is not divisible by $exp(G)$, then $G = G^d$. So, every element of G can be expressed both, as a product of a finite number of commutators in G and as a product of finitely many p-th powers in G. But the existence of a bound for the number of factors in any element of G has important consequences, for instance in profinite groups.

In 1996, C. Martínez and E. Zelmanov [12] proved that for a natural number $d \geq 1$, there exists a function $N(d)$ such that for an arbitrary simple group G either $G^d = 1$ or $G = \{a_1^d ... a_N^d \mid a_i \in G\}$.

In particular, for alternating groups A_n, $n \geq 5$, Martínez and Zelmanov used a result by Bertran that says that any even permutation in A_n can be written as a product of two cycles, each one of length l, if and only if, $[3n/4] \leq l \leq n$..

Clearly, it seems that the bound depends on d. For instance, if $d = 2$ every element in A_n, $n \geq 5$, is a product of two squares in A_n. However, if $d = 210$, it is impossible to write every 7-cycle in A_7 as a product of two 210-th powers in A_7. But, for every natural number $m' < 210$, it can be proved that every element in A_7 can be written as a product of two m'-th powers.

Still, it is natural to ask if we can find a general constant N such that every element in an alternating group A_n, $n \geq 5$, can be written as a product of N d-th powers of elements in A_n. In this paper it is proved that this is the case for $d = p^r$, where p is a prime number and r is a natural number. And in this case, $N = 2$.

These ideas can be reformulated in an slightly different way. Given an arbitrary group G and a word in the free group of rank r, $\omega \in \mathbb{F}_r$, with r a natural number, we can consider the word map $\omega : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$ that maps each tuple $(g_1, g_2, ..., g_r)$ to $\omega(g_1, g_2, ..., g_r)$. It has sense to ask if this word map is surjective.

Of course, there are words for which $\omega(G) \neq G$. For example, the word x^2 is not surjective on any finite non abelian simple group. Nevertheless, some word maps are surjective, and it is an interesting problem in Group Theory to determine which ones are.

The first non-trivial example of a word map which is surjective on all finite non-abelian simple groups is the commutator map $[x, y]$. It was proved in [8], giving a positive answer to a conjecture formulated by Ore, who had proved in 1951 [13] the result for alternating groups.

In [11] authors proved in the same article that every element of a sufficiently large finite simple group is a product of two squares and posed the conjecture that the word x^2y^2 is surjective . This conjecture was proved in [9], where authors also proved that if $p > 7$ is a prime number, then any element of a finite non-abelian simple group G is a product of two p-th powers.

At the same time, R. Guralnick and G. Mall got a new proof using some results about conjugacy classes. In [6], they proved that there always exist two conjugacy classes in a finite non abelian simple group such that every non trivial element of the group belongs to the product of these conjugacy classes. This result is used to prove that every element in a finite non abelian simple group can be written as a product of two p^k-th powers, with p a primer number.

We must emphasize that the proof of all these results is highly nontrivial. Our aim here is to show a proof of the mentioned result for alternating groups

A_n, $n \geq 5$, that uses only elementary techniques.

Let's mention an elementary fact that will be extensively used in what follows. Given a group G and a natural number $n \geq 1$, the mapping

$$\begin{aligned} \varphi_n : G &\longrightarrow G \\ g &\mapsto g^n \end{aligned}$$

is bijective if an only if the greatest common divisor $gcd(n, exp(G)) = 1$.

Indeed, if we take a prime divisor p of $exp(G)$ and n, there exists an element in $g \in G$ of order p. So $\varphi(g) = \varphi(1) = 1$.

The next elementary result will very useful in this paper.

Theorem 1.1. *If G is a finite group, g is an element of G and $d \geq 1$ is an integer such that $gcd(o(g), d) = 1$, then $g = (g^s)^d$ for some integer $s \geq 1$.*

Proof. It suffices to consider the cycle group $\langle g \rangle$. As the $gcd(o(g), d) = 1$, we can apply the Bezout's Identity to get that there exist $t, s \in \mathbb{Z}$ such that $1 = o(g)t + sd$.

Then we have that

$$g = g^{o(g)t+sd} = g^{o(g)t} g^{sd} = (g^s)^d.$$

□

In order to address our problem and study p^k-th powers in A_n, we will distinguish 3 different cases: $p = 2$, $p = 3$ and $p > 3$.

Before starting, we want to give an elementary definiton.

Definition 1.1. *Let σ be a permutation of a symmetric group S_n, $n \geq 1$. The support of σ is defined as*

$$supp(\sigma) = \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}.$$

The following results will be an essential tool in the paper.

Lemma 1.2. *Let m be a positive integer and $n \geq 5$. Take $\sigma_1, ..., \sigma_k$ permutations in A_n such that $\sigma_i = \lambda_i^m$ for some $\lambda_i \in A_n$. If $supp(\sigma_i) \cap supp(\sigma_j) = \emptyset$ for every $i \neq j$, then there exists $\lambda \in A_n$, such that $\sigma_1 ... \sigma_k = \lambda^m$ and*

$$supp(\lambda) = \bigcup_{i=1}^{k} supp(\sigma_i).$$

Proof. For each $i \in \{1, ..., k\}$, we have that there exists $\lambda_i \in A_n$ such that $\sigma_i = \lambda_i^m$.

We can assume, without loss of generality that $supp(\lambda_i) = supp(\sigma_i)$, and so, the supports of λ_i and λ_j are disjoint for every $i \neq j$ and we have that λ_i commutes with λ_j for every $i \neq j$.

Then, we have that

$$\prod_{i=1}^{k} \sigma_i = \prod_{i=1}^{k} (\lambda_i)^m = (\prod_{i=1}^{k} \lambda_i)^m.$$

It is enough to take $\lambda = \prod_{i=1}^{k} \lambda_i$.
Let us notice that $supp(\lambda) = \bigcup_{i=1}^{k} supp(\sigma_i)$.

□

Theorem 1.3. *Let $\sigma_1, ..., \sigma_t$ permutations in A_n such that $\sigma_i = \lambda_{i1}^d ... \lambda_{iN}^d$ for some $N, d \geq 1$. If σ_i and σ_j are disjoint when $i \neq j$ and $supp(\sigma_i) = \cup_{j=1}^{N} supp(\lambda_{ij})$, then there exist permutations $\lambda_1, ..., \lambda_N$ such that*

$$\sigma_1 ... \sigma_t = \lambda_1^d ... \lambda_N^d.$$

Proof. It suffices to take $\lambda_1 = \lambda_{11} ... \lambda_{t1}$,..., $\lambda_N = \lambda_{1N} ... \lambda_{tN}$ and take into account that λ_{ij} commutes with λ_{hl} if $i \neq h$. Then, we can use Lemma 1.2 to get the result.

Notice that again $\cup_{i=1}^{N} supp(\lambda_i) = \cup_{j=1}^{t} supp(\sigma_j)$. □

In this paper n will be an integer greater than or equal to 5 and k will be an integer greater than or equal to 1.

The main result of this paper is the next theorem.

Theorem 1.4. *Let p be a prime number. Every element in an alternating group A_n can be written as a product of two p^k-th powers in A_n.*

2 The case $p = 2$

We will start with the case of $p = 2$. We will consider first those permutations of A_n that can be written as products of cycles of odd length.

Lemma 2.1. *Let σ be a permutation that can be written as a product of disjoint cycles of odd length. Then there exists λ in A_n such that $\sigma = \lambda^{2^k}$.*

Proof. Suppose that $\sigma = (a_1, ..., a_k)$ is a cycle of length odd, $k \geq 3$.

Since $gcd(2, o(\sigma)) = 1$, we can apply Lemma 1.1 to get that $\sigma = (\sigma^s)^{2^k}$ for some $s \geq 1$. Clearly, $supp(\sigma) = supp(\sigma^s)$. □

Lemma 2.2. *Let σ be a permutation in A_n that can be written as a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{2^k} \eta^{2^k}$.*

Proof. Suppose initially that $\sigma = (a_1, ..., a_{2i})(a_{2i+1}, ..., a_{2r})$ is a permutation in A_n that is a product of two cycles of even length. It is enough to rewrite σ as $\sigma = \xi_1\eta_1$, where $\xi_1 = (a_1, a_2, ..., a_{2i+1})$ and $\eta_1 = (a_{2i}, a_{2i+1}, ..., a_{2r})$.

By Lemma 2.1 there exist elements ξ and η in A_n such that $\xi_1 = \xi^{2^k}$, $\eta_1 = \eta^{2^k}$. So

$$\sigma = \xi^{2^k}\eta^{2^k}.$$

Notice that we can always assume that $supp(\xi), supp(\eta) \subset supp(\sigma)$.

Lemma 2.2 is now a direct consequence of Lemma 2.1. □

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 2.1 and σ_2 satisfies the assumptions of Lemma 2.2, a direct application of Theorem 1.3 gives Theorem 1.4 in the case $p = 2$.

3 The case $p \geq 5$

In this section we will address the case $p \geq 5$. We will start considering cycles of odd length.

Lemma 3.1. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length, then there exist λ and μ in A_n such that $\sigma = \lambda^{p^k}\mu^{p^k}$.*

Proof. Let's consider first the case in which σ is a single cycle. Suppose that $\sigma = (a_1, ..., a_r)$, with $r \geq 3$ odd. We will distinguish two different cases:

- If p is not a divisor of $o(\sigma)$, the result follows from Lemma 2.1, since $\sigma = (\sigma^s)^{p^k}$ for some integer s.
- If p is a divisor of $o(\sigma)$, then we can rewrite σ as

  $$\sigma = (a_1, a_2, a_3)(a_3, a_4, ..., a_r)$$

  as a product of a 3-cycle and a $(r-2)$-cycle.

  But p does not divide neither to 3 nor to $(r-2)$. So, using the previous case, there exist α and β elements in A_n such that

  $$(a_1, a_2, a_3) = \alpha^{p^k} \quad \text{and} \quad (a_3, ..., a_r) = \beta^{p^k}.$$

  So

  $$\sigma = (a_1, a_2, a_3)(a_3, a_4, ..., a_r) = \alpha^{p^k}\beta^{p^k}.$$

Notice that $supp(\alpha), supp(\beta) \subset supp(\sigma)$

Theorem 1.3 immediately extends the previous result to permutations that are product of disjoint cycles of odd length.

□

Now, let's consider products of disjoint cycles of even length.

Lemma 3.2. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then σ can be written as a product of two p^k-th powers in $A_{supp(\sigma)}$.*

Proof. To start, consider $\sigma = \sigma_1\sigma_2$ a permutation in A_n, where $\sigma_1 = (a_1, ..., a_{2i})$ and $\sigma_2 = (a_{2i+1}, ..., a_{2r})$. We will consider two different cases:

- If p is not a divisor of $o(\sigma)$, by Lemma 1.1, we have that $\sigma = (\sigma^s)^{p^k}$ for some $s \geq 1$.
- If p is a divisor of $o(\sigma)$, let's distinguish two different cases:
  1. If p divides both $o(\sigma_1)$ and $o(\sigma_2)$, then we can rewrite σ as follows:

     $$\sigma = (a_1, a_2)(a_{2i+1}, a_{2i+2})(a_2, ..., a_{2i})(a_{2i+2}, ..., a_{2r}).$$

     Denoting $(a_1, a_2)(a_{2i+1}, a_{2i+2}) = \lambda_1$ and $(a_2, ..., a_{2i})(a_{2i+2}, ..., a_{2r}) = \lambda_2$, it is clear that $\lambda_1 = \lambda_1^{p^k}$ because of $o(\lambda_1) = 2$.
     On the other hand, we have that p is neither a divisor of $o(\sigma_1) - 1$ nor of $o(\sigma_2) - 1$. So, by Lema 1.1, we have that λ_2 is a p^k-th power in A_n.
     That is, there exist permutations λ and μ in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$. So

     $$\sigma = \lambda^{p^k}\mu^{p^k}.$$

  2. Suppose that p is a divisor of $o(\sigma_2)$ and not of $o(\sigma_1)$ (the case $p \mid o(\sigma_1)$ and $p \nmid o(\sigma_2)$ is similar). We can rewrite σ as

     $$\sigma = \sigma_1(a_{2i+1}, a_{2i+2})(a_{2i+2}, ..., a_{2r}).$$

     Denoting $\lambda_1 = \sigma_1(a_{2i+1}, a_{2i+2})$ and $\lambda_2 = (a_{2i+2}, ..., a_{2r})$, we have that p is not a divisor of $o(\lambda_1)$ and that p is not a divisor of $o(\lambda_2) = o(\sigma_2) - 1$.
     So, applying Lemma 1.1 to λ_1 and to λ_2 we have that there exist λ and μ permutations in A_n such that $\lambda_1 = \lambda^{p^k}$, $\lambda_2 = \mu^{p^k}$.
     So, we have that

     $$\sigma = (\lambda)^{p^k}(\mu)^{p^k}.$$

□

Since every even permutation σ in A_n can be written as a product of two disjoint permutations $\sigma = \sigma_1\sigma_2$, where σ_1 satisfies the assumptions of Lemma 3.1 and σ_2 satisfies the assumptions of Lemma 3.2, a direct application of Theorem 1.3 gives Theorem 1.4 in the case $p \geq 5$.

4 The case $p = 3$

We will prove that for every natural number $k \geq 1$, every element in A_n, can be written as a product of two 3^k-th powers.

Let's start with the study of cycles of odd length.

Lemma 4.1. *Every cycle σ in A_n with odd length $s \geq 3$ can be written as a product of two 3^k-th powers in A_n*

Proof. Take $\sigma = (a_1, ..., a_s)$, with $s \geq 3$ odd. We distinguish three different cases:

1. If 3 does not divide to $o(\sigma)$ we can apply Lemma 1.1 to get that $\sigma = (\sigma^t)^{3^k}$ for some $t \geq 1$.

2. If $3 \mid o(\sigma) = s$ and $s \geq 9$, we can rewrite σ as a product of two cycles

$$\sigma := (a_1, ..., a_5)(a_5, ..., a_s),$$

one of length 5 and the other one of length $s - 4$. Clearly 3 does not divide $s - 4$.

Denoting $\lambda_1 = (a_1, ..., a_5)$ and $\lambda_2 = (a_5, ..., a_s)$, we have that $\lambda_1 = (\lambda_1^r)^{3^k}$ and $\lambda_2 = (\lambda_2^t)^{3^k}$ for some $r, t \geq 1$.

So,

$$\sigma = (\lambda_1^r)^{3^k}(\lambda_2^t)^{3^k}.$$

Notice that $\lambda_1, \lambda_2 \in A_{supp(\sigma)}$.

3. Suppose $s = 3$. Assume $\sigma = (a_1, a_2, a_3)$ and take the permutation $x := (a_1, a_5, a_3, a_4, a_2)$ and $y := (a_1, a_3, a_5, a_2, a_4)$ in A_n (Remember that $n \geq 5$). Then we have that $\sigma = yx$, and, by the first case, there exist λ_1 and λ_2 in A_n such that $x = \lambda_1^{3^k}$ and $y = \lambda_2^{3^k}$, that is

$$\sigma = \lambda_2^{3^k}\lambda_1^{3^k}.$$

□

Remark: If σ is a 3-cycle, $A_{supp(\sigma)} \simeq A_3 \leq A_4$, it is impossible to write σ as a product of two 3^k-th powers neither in A_3 nor A_4.

Indeed, A_3 is an abelian group of order 3 and $A_4^3 = V$, where V is the 4-Klein group that consists of the identity and all products of two disjoint transpositions.

We will need, at least, 5 symbols to write a 3-cycle as a product of two 3^k-powers, for every $k \geq 1$. That's why we have to be careful when using Lemma 1.2, in case that a 3-cycle is involved in a permutation σ.

The problem does not appear if only cycles of odd length greater than or equal to 5 appear.

Corollary 4.2. *Let σ be a permutation in A_n that can be written as a product of disjoint cycles of odd length greater than 3. Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Lemma 4.3. *Let σ be a permutation in A_n that is a product of r disjoint 3-cycles, $r \geq 2$. Then there exist λ and μ in $A_{supp(\sigma)}$ such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Proof. Suppose $\sigma = \sigma_1...\sigma_r$, such that σ_i is a 3-cycle for every $i \in \{1, ..., r\}$, $r \geq 2$ and σ_i, σ_j disjoint if $i \neq j$.

- If $r = 2$, suppose that

  $$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6).$$

  Then σ can be rewritten as

  $$\sigma = \xi_1\xi_2,$$

  where $\xi_1 = (a_1, a_2)(a_4, a_5)$ and $\xi_2 = (a_2, a_3)(a_5, a_6)$.
  Since $o(\xi_1) = 2 = o(\xi_2)$ it follows from Lemma 1.1 that

  $$\sigma = (\xi_1^{s_1})^{3^k}(\xi_2^{s_2})^{3^k}.$$

  Notice that $\xi_1, \xi_2 \in A_{supp(\sigma)}$.

- For r even, the result follows immediately from Theorem 1.3 and the case $r = 2$.

- If $r = 3$,

  $$\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)(a_7, a_8, a_9).$$

  Now, we can rewrite $\sigma = \lambda_1\lambda_2$, with $\lambda_1 = (a_1, a_6, a_9, a_5, a_8, a_2, a_3)$ and $\lambda_2 = (a_1, a_8, a_6, a_4, a_9, a_7, a_5)$.
  Since $o(\lambda_1) = 7 = o(\lambda_2)$, by Lemma 1.1 $\lambda_1 = (\lambda_1^{l_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{l_2})^{3^k}$. So

  $$\sigma = (\lambda_1^{l_1})^{3^k}(\lambda_2^{l_2})^{3^k}.$$

  Notice that $\lambda_1, \lambda_2 \in A_{supp(\sigma)}$.

- If r is odd, $r \geq 5$, then we can consider the product of the first three 3-cycles and the rest of the 3-cycles in pairs.

  Now the result for σ follows immediately from Theorem 1.3 and the previous cases.

□

Lemma 4.4. *Let σ be a permutation that is a product of disjoint cycles of odd length.Then there exist λ and μ in A_n such that $\sigma = \lambda^{3^k}\mu^{3^k}$.*

Proof. If at least two 3-cycles appear, it follows from Theorem 1.3 and Lemmas 4.1 and 4.3. So let us assume that only one 3-cycle appears, in the expression of σ as product of cycles of odd length.

Let's write $\sigma = \sigma_1\alpha_1...\alpha_r$, with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_i a cycle of odd length greater than 3 for every $i \in \{1, ..., r\}$.

We can apply Lemma 4.1 and Theorem 1.3 to $\alpha_2...\alpha_r$ to get that there exist β, γ in A_n such that $supp(\beta, \gamma) \subset \cup_{i=2}^{r} supp(\alpha_i)$ such that

$$\alpha_2...\alpha_r = \beta^{3^k}\gamma^{3^k}.$$

Consider now $\sigma_1\alpha_1 = (a_1, a_2, a_3)(a_4, a_5, ..., a_s)$, with $s \geq 8$ even. We distinguish two cases:

- If 3 does not divide to $s - 4$, we can rewrite $\sigma_1\alpha_1$ as follows:

  $$\sigma_1\alpha_1 = (a_1, a_2)(a_4, a_5)(a_2, a_3)(a_5, ..., a_s).$$

  If we denote $\lambda_1 = (a_1, a_2)(a_4, a_5)$ and $\lambda_2 = (a_2, a_3)(a_5, ..., a_s)$, we have that 3 does not divide neither to $o(\lambda_1) = 2$ nor to $o(\lambda_2) = s - 4$.

  By Lemma 1.1, $\lambda_1 = (\lambda_1^{m_1})^{3^k}$ and $\lambda_2 = (\lambda_2^{m_2})^{3^k}$, for some $m_1, m_2 \geq 1$.

  So, we have that

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

- If 3 is a divisor of $s - 4$, we can rewrite $\sigma_1\alpha_1$ as follows:

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2,$$

  where $\lambda_1 = (a_1, a_2, a_3, a_4, a_5)$ and $\lambda_2 = (a_3, a_5, a_6, ..., a_s)$. Then 3 does not divide neither to $o(\lambda_1) = 5$ nor to $o(\lambda_2) = (s - 3)$.

  Again by Lemma 1.1 we get that $\lambda_1 = (\lambda_1^{n_1})^{3^k}$ and that $\lambda_2 = (\lambda_2^{n_2})^{3^k}$, for some $n_1, n_2 \geq 1$.

  Consequently

  $$\sigma_1\alpha_1 = \lambda_1\lambda_2 = (\lambda_1^{m_1})^{3^k}(\lambda_2^{m_2})^{3^k}.$$

  Theorem 1.3 finishes the proof of this Lemma.

□

It remains to consider products of cycles of even length.

Lemma 4.5. *Let σ be a permutation in A_n that is a product of an even number of disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof. The proof follows the same lines of the proof of Lemma 3.2. □

If σ is a permutation in A_n, we can write it as

$$\sigma = \sigma_1 ... \sigma_r \gamma_1 ... \gamma_s (\alpha_1\alpha_2)...(\alpha_{2l-1}\alpha_{2l}),$$

where each σ_i is a 3-cycle, $i \in \{1, ..., 2r\}$, γ_j is a cycle of odd length greater or equal than 5, $j \in \{1, ..., s\}$, and α_k is a cycle of even length for every k, $k \in \{1, ..., 2l\}$.

Theorem 1.4 follows from Theorem 1.3 together with Lemmas 4.3 and 4.4 except in the case $s = 0$, $r = 1$ and $l \geq 1$. Notice that in this case σ_1 is a product of two 3^k-powers, but we need to involve two symbols that do not appear in $supp(\sigma_1)$, so Theorem 1.3 can not be directly applied.

To finish the result we only need the following Lemma.

Lemma 4.6. *Let σ be a permutation in A_n that is a product of a single 3-cycle and two disjoint cycles of even length. Then there exist μ, η in A_n such that $\sigma = \mu^{3^k}\eta^{3^k}$.*

Proof. Suppose that σ can be written as follows:

$$\sigma = \sigma_1(\alpha_1\alpha_2),$$

with $\sigma_1 = (a_1, a_2, a_3)$ a 3-cycle and α_1, α_2 are cycles of even length, $\alpha_1 = (b_1, ..., b_{2i})$, $\alpha_2 = (b_{2i+1}, ..., b_{2t})$.

We distinguish four different cases:

- If 3 divides to both $o(\alpha_1)$ and $o(\alpha_2)$, or equivalently $3 \mid i$ and $3 \mid t$, we rewrite σ as $\sigma = \lambda_1\lambda_2$, where $\lambda_1 = (a_1, a_2)(b_1, b_2)(b_{2i+1}, ..., b_{2t-1})$ and $\lambda_2 = (a_2, a_3)(b_{2t-1}, b_{2t})(b_2, ..., b_{2i})$.

  But 3 does not divide neither to $o(\lambda_1) = 2(2(t-i)-1)$ nor to $o(\lambda_2) = 2(2i-1)$. So Lemma 1.1 gives the result, since $\lambda_1 = (\lambda_1^p)^{3^k}$ and $\lambda_2 = (\lambda_2^q)^{3^k}$, for some $p, q \in \mathbb{Z}$.

- If 3 divides to $o(\alpha_1)$ but does not divide to $o(\alpha_2)$, that is $3 \mid i$, but $3 \nmid t$, we rewrite σ as follows:

  $$\sigma = \lambda_1\lambda_2,$$

  where $\lambda_1 = (a_1, a_2, a_3, b_1)(b_{2i+1}, ..., b_{2t})$ and $\lambda_2 = (a_3, b_1, b_2, ..., b_{2i})$.

  Now, 3 does not divide to $(2i+1) = o(\lambda_2)$, so we can apply Lemma 1.1.

  Similarly, 3 does not divide to $4(t-i) = o(\lambda_1)$. we can use again Lemma 1.1.

So,

$$\sigma = (\lambda_1^v)^{3^k}(\lambda_2^u)^{3^k},$$

for some integers u, v.

- If 3 divides to $o(\alpha_2)$ but 3 does not divide to $o(\alpha_1)$, the proof is similar.
- If 3 does not divide neither to $o(\alpha_2)$ nor to $o(\alpha_1)$, we rewrite σ as follows

$$\sigma = (a_1, a_2, a_3, b_1, b_2)(a_3, b_2, ..., b_{2i})(b_{2i+1}, ..., b_{2t}).$$

Denote $\lambda_1 = (a_1, a_2, a_3, b_1, b_2)$ and $\lambda_2 = (a_3, b_2, ..., b_{2i})(b_{2i+1}, ..., b_{2t})$.

Since 3 does not divide to $o(\lambda_1) = 5$ and 3 does not divide to $o(\lambda_2) = mcm(2i, 2t - 2i)$, the result follows immediately from Lemma 1.1.

This finishes the proof of Lemma 4.6 and gives Theorem 1.4 in the case $p = 3$.

□

Acknowledgements

This work was partially supported by BES-2011-044790 (research fellowship associated to project MTM2010-18370-C04-01).

References

[1] E. Bertran, *Even Permutations as a Product of Two Conjugate Cycles.* Journal of Combinatorial Theory 12: 368-380.

[2] E. Bertran, *Powers of Cycle-Classes in Symmetric Groups.* Journal of Combinatorial Theory 94: 87-99.

[3] V. I. Chernousov, E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part: short proof.* J. Algebra 229 (2000), no. 1, 314-332.

[4] E. W. Ellers and N. L. Gordeev, *On the conjectures of J. Thompson and O. Ore.* Trans. Amer. Math. Soc. 350 (1998), no. 9, 3657-3671

[5] W. J. Ellision, *Warings's Problem.* American Mathematical Monthly 78: 10-36.

[6] R. Guralnick and G. Malle, *Products of conjugacy classes and fixed point spaces.* J. Amer. Math. Soc. 25 (2012), no. 1, 77-121.

[7] M. Larsen and A. Shalev, *World maps and Waring type problems*. Journal of the Amer. Math. Soc. 22: 437-466.

[8] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep. *The Ore Conjecture*. J. Eur. Math. Soc. 12: 939-1008

[9] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep. *Products of squares in finite simple groups*. Amer. Math. Soc. 140 (2012), no. 1 Pages 21-33

[10] M. W. Liebeck and A. Shalev, *Diameter of simple groups: sharp rounds and applications*. Annals of Math. 154: 383-406.

[11] M. J. Larsen, A. Shalev and P. H. Tiep, *The Waring problem for finite simple groups*. Ann. of Math. (2) 174 (2011), no. 3, 1885-1950.

[12] C. Martinez and E. I. Zelmanov, *Product of powers in finite simple groups*. Israel J. Math. 96: 469-479.

[13] O. Ore, *Some Remarks on Commutators*. Proc. Amer. Math. Soc. 2: 307-314.

[14] J. Saxl and J. S. Wilson, *A note on powers in simple groups*, Math. Proc. Camb. Phil. Soc. 122: 91-94.

[15] J. S. Wilson, *First-order group theory*. Infinite Groups (1994). Gruyter, Berlin, 1996, pp. 301-314.

Título: Engel Words in Alternating Groups.
Autor: Jorge Martínez Carracedo.
Revista de publicación: Journal of Algebra and Its Applications (2016).

Journal of Algebra and Its Applications

ENGEL WORDS IN ALTERNATING GROUPS

JORGE MARTÍNEZ CARRACEDO
Departamento de Matemáticas
Universidad de Oviedo.
C/ Calvo Sotelo, s/n, 33007 Oviedo.
Spain.
martinezjorge@uniovi.es

Received (Day Month Year)
Revised (Day Month Year)
Accepted (Day Month Year)

Communicated by (xxxxxxxxx)

In this paper we prove that every element in the alternating group A_n, with $n \geq 5$, can be written as a product of at most two Engel words of arbitrary length.

Keywords: Simple groups; Alternating groups; Engel words; Verbal subgroup.

2000 Mathematics Subject Classification: 20D05, 20D06, 20B35.

1. Introduction

Given an arbitrary group G and a word in the free group of rank r, $\omega \in \mathbb{F}_r$, with r a natural number, we can consider the word map

$$\omega : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$$

that maps each tuple $(g_1, g_2, ..., g_r)$ to $\omega(g_1, g_2, ..., g_r)$.

Several questions can be formulated: What is the size of the set $\omega(G)$? Is the map ω surjective? Is it $\langle \omega(G) \rangle = G$? Can we find a constant k for which $\omega(G)^k = \langle \omega(G) \rangle$? The group $\langle \omega(G) \rangle$ is defined as the verbal subgroup generated by the word ω. We refer the reader to [9] for further information.

We can see some similarities between the last question and Waring's Problem (see [1] and [5]), so the aforementioned problem can be thought as an analogous of Waring's Problem in a non-commutative frame.

O. Ore published in 1951 [7] a result proving that every element of an alternating group A_n, with $n \geq 5$, can be written as a commutator of elements in A_n.

Notice that Ore's result says that if we take the word $\tau := x_1^{-1} x_2^{-1} x_1 x_2$ in the free group of rank 2, $\mathbb{F}_2$, then $\tau(A_n) = A_n$, for all $n \geq 5$. Furthermore, he

conjectured that the result is also true for any finite simple group G, what is known as the Abstract Ore Conjecture.

In 1994, Wilson [10], got a first progress in this problem. He proved that for any finite simple group, there exists a constant k such that, $\tau(G)^k = G$.

On the other side, some results were obtained considering the word $\xi := x^n$, with n a natural number. In 1996, Martínez and Zelmanov [6] and in 1997, Saxl and Wilson [8] proved, independently, that for every finite simple group big enough, there exists a constant k such that $\xi(G)^k = G$.

In 2001 Liebeck and Shalev [4] got an important breakthrough when they proved that for every word $\omega \neq 1$ there exists a positive integer $N = N(\omega)$ such that for every finite simple group G, with $|G| \geq N(\omega)$, we have that

$$\omega(G)^3 = G.$$

In 2008, Larsen and Shalev [2] improved this result proving that the exponent 3 can be replaced by 2, in some families of finite simple groups.

Finally, in 2010, M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep [3] finished the proof of the Ore Conjecture. They proved that for every finite simple group G, $G = \tau(G)$, where $\tau := x_1^{-1}x_2^{-1}x_1x_2$ denotes the commutator. The proof of this result is highly non trivial and uses theory of characters and deep computations with algebraic computer programs specially designed.

What happens if we consider Engel words of arbitrary length, $E_m = [...[x, y], y], ..., y]$, instead of the commutator τ? Is it still true that $G = E_m(G)$ for every finite simple group G and any natural number m?

Our aim in this paper is to give a first answer for alternating simple groups. We will prove that every element in A_n, with $n \geq 5$, can be written as a product of at most two Engel words of arbitrary length, that is

$$A_n = E_m(A_n)E_m(A_n),$$

for any natural numbers $m \geq 2$ and $n \geq 5$.

We would like to remark that only elementary techniques of Group Theory are used in this paper and that this result is not a particular case of the one proved by Larsen and Shalev [2] for alternating groups, since their result is proved for big enough orders.

2. Preliminary results

Let us consider a natural number r and the associated free group of rank r, $\mathbb{F}_r$. Let ω be a reduced word of $\mathbb{F}_r$. We can define the word map as

$$\begin{aligned} \omega : \overbrace{G \times \cdots \times G}^{r} &\longrightarrow G \\ (g_1, ..., g_r) &\mapsto \omega(g_1, ..., g_r) \end{aligned}$$

which allows us to give the next definition.

Definition 2.1. Given a reduced word ω in the free group of rank r, $\mathbb{F}_r$, G a group and $\omega : \overbrace{G \times \cdots \times G}^{r} \longrightarrow G$, the verbal subgroup of G associated with ω is defined as the group generated by the set $\omega(G) := \{\omega(g_1, ..., g_r) \mid g_1, ..., g_r \in G\}$.

Definition 2.2. Let m be a positive integer. An Engel word of length m is defined as the element of $\mathbb{F}_2$

$$E_m = [...[x, \overbrace{y], y], ..., y}^{m}].$$

If G is a group, the verbal subgroup of G associated with the Engel word of length m, $< E_m(G) >$, is called Engel subgroup of length m.

Before starting with the study of the problem, we need some preliminary results that will be instrumental in this paper because under certain conditions, they tell us that the product of two Engel words of arbitrary length is actually a single word of the same length.

In this paper n will be an integer greater than or equal to 5 and, when it is used, m will be an integer greater than or equal to 2.

Lemma 2.1. *Let $\sigma_1, \sigma_2, \sigma_3$ and σ_4 be permutations in S_n such that σ_1, σ_2 commute with σ_3, σ_4. Then, for all $m \in \mathbb{N}$, we have*

$$E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) = E_m(\sigma_1, \sigma_2)E_m(\sigma_3, \sigma_4).$$

Proof. Since σ_1, σ_2 commute with σ_3, σ_4, we have that every element in the group $\langle \sigma_1, \sigma_2 \rangle$ commutes with every element in the group $\langle \sigma_3, \sigma_4 \rangle$. In particular, $[\sigma_1, \sigma_2]$ commutes with $[\sigma_3, \sigma_4]$ and $E_2(\sigma_1, \sigma_2)$ commute with $E_2(\sigma_3, \sigma_4)$.

On the other hand,

$$[\sigma_1\sigma_3, \sigma_2\sigma_4] = \sigma_3^{-1}\sigma_1^{-1}\sigma_4^{-1}\sigma_2^{-1}\sigma_1\sigma_3\sigma_2\sigma_4 = \sigma_3^{-1}\sigma_4^{-1}\sigma_3\sigma_4\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 =$$

$$= [\sigma_3, \sigma_4][\sigma_1, \sigma_2] = [\sigma_1, \sigma_2][\sigma_3, \sigma_4].$$

Therefore,

$$E_2(\sigma_1\sigma_3, \sigma_2\sigma_4) = [[\sigma_1\sigma_3, \sigma_2\sigma_4], \sigma_2\sigma_4] = [[\sigma_1, \sigma_2][\sigma_3, \sigma_4], \sigma_2\sigma_4],$$

and $[\sigma_1, \sigma_2]$ and σ_2 commute with $[\sigma_3, \sigma_4]$ and σ_4. Applying the above argument, we can write that:

$$E_2(\sigma_1\sigma_3, \sigma_2\sigma_4) = [[\sigma_1, \sigma_2], \sigma_2][[\sigma_3, \sigma_4], \sigma_4] = E_2(\sigma_1, \sigma_2)E_2(\sigma_3, \sigma_4).$$

So, by induction if the result is true for $m - 1$, that is

$$E_{m-1}(\sigma_1\sigma_3, \sigma_2\sigma_4) = E_{m-1}(\sigma_1, \sigma_2)E_{m-1}(\sigma_3, \sigma_4).$$

So, we have that

$$E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) = [E_{m-1}(\sigma_1\sigma_3, \sigma_2\sigma_4), \sigma_2\sigma_4] = [E_{m-1}(\sigma_1, \sigma_2)E_{m-1}(\sigma_3, \sigma_4), \sigma_2\sigma_4],$$

and, as $E_{m-1}(\sigma_1, \sigma_2)$ and σ_2 commute with $E_{m-1}(\sigma_3, \sigma_4)$ and σ_4, we have that

$$\begin{aligned} E_m(\sigma_1\sigma_3, \sigma_2\sigma_4) &= [E_{m-1}(\sigma_1, \sigma_2)E_{m-1}(\sigma_3, \sigma_4), \sigma_2\sigma_4] = \\ &= [E_{m-1}(\sigma_1, \sigma_2), \sigma_2][E_{m-1}(\sigma_3, \sigma_4), \sigma_4] = \\ &= E_m(\sigma_1, \sigma_2)E_m(\sigma_3, \sigma_4). \end{aligned}$$

□

Corollary 2.1. *Let $\sigma_1, ..., \sigma_{2r}$ be permutations in S_n such that σ_{2i-1} commutes with σ_j for every $j \neq 2i$ and σ_{2i} commutes with σ_j for every $j \neq 2i-1$. Then, for all $m \in \mathbb{N}$, we have that*

$$E_m(\sigma_1\sigma_3...\sigma_{2r-1}, \sigma_2\sigma_4, ..., \sigma_{2r}) = E_m(\sigma_1, \sigma_2)E_m(\sigma_3, \sigma_4)...E_m(\sigma_{2r-1}, \sigma_{2r}).$$

Proof. It is sufficient to use Lemma 2.1. □

Let's denote for a permutation τ in a symmetric group S_n, its support as

$$supp(\tau) := \{i \in \{1, ..., n\} \mid \tau(i) \neq i\}.$$

Clearly τ can be seen as a permutation in $S_{supp(\tau)}$. It is clear that if σ is a permutation in S_n that can be written as an Engel word (resp. a product of two Engel words) in A_n, then the same is true in A_m, with $m > n$.

The main result of this paper is the following:

Theorem 2.1. *Every permutation in A_n can be written as a product of two Engel words of arbitrary length m in A_n.*

3. The case $m = 2$

In the first part of this paper we will prove that every element in an Alternating Group A_n, $n \geq 5$, can be written as a product of two Engel words of length two.

Remark. Given σ an even permutation, $\sigma = \sigma_1...\sigma_t$ its decomposition as a product of disjoint cycles. We will consider the following four types:

1. Every σ_i is a cycle of odd length greater than 3.
2. Every σ_i is a cycle of odd length and there exist $r \geq 2$ 3-cycles.
3. $t = 2s$ and the length of σ_i is even for every $i \in \{1, ..., 2s\}$.
4. There is exactly one 3-cycle, σ_i.

Notice that every even permutation can be expressed as a disjoint product of permutations of the previous types. Let's consider first a permutation σ that is is a product of two 2-cycles.

Lemma 3.1. *Let $\sigma = (a, d)(b, c)$ be a permutation in $A_4 \subset A_n$. Then σ is an Engel word of length two in $A_4 \subset A_n$.*

Proof. It is enough to take $\tau = (a, c, b)$ and $\zeta = (a, d, b)$. It is easy to show that $(a, d)(b, c) = E_2(\tau, \zeta)$. □

Next lemma deals with cycles in A_n. Note that any cycle in A_n has an odd length.

Lemma 3.2. *Let p be an odd number, $p \geq 3$ and σ a p-cycle in A_p. Then σ is an Engel word of length two in S_p, and so, in A_{p+2}.*

Proof. Without loss of generality, we can suppose that $\sigma := (1, ..., p)$.

Since $\#supp(\sigma) = p$, we can consider $\sigma \in A_p$. We know that $o(\sigma) = p$ and $(2, p) = 1$, so σ^2 is also a p-cycle. We conclude that σ and σ^2 are conjugated in S_p.

Hence, there exists a permutation τ in S_p such that $\sigma^\tau = \sigma^2$, that is, $[\sigma, \tau] = \sigma$, and $\sigma = E_2(\sigma, \tau)$. Now it is enough to use the well known embedding of S_p in A_{p+2}, that is:

If $\tau \in A_p \subset A_n$, we have obtained $\sigma \in E_2(A_p)$.

If $\tau \in S_p \setminus A_p$, we consider the permutation $\zeta = \tau(p + 1, p + 2) \in A_{p+2}$ and $\sigma = E_2(\sigma, \zeta) \in E_2(A_{p+2})$. □

Lemma 3.3. *Let p be an odd number, $p \geq 5$. Every p-cycle can be written as a product of two Engel words of length two in A_p.*

Proof.

We can suppose $\sigma = (1, ..., p)$ as before. Then, $\sigma = \sigma_1\sigma_2$, with $\sigma_1 = (1, 2, 3)$ and $\sigma_2 = (3, 4, ..., p)$. We would like to emphasize that $\sigma_1, \sigma_2 \in A_p$ are both cycles of length greater or equal than 3.

According to Lemma 3.2, there exist $\tau_1 \in S_{\{1,2,3\}}$ and $\tau_2 \in S_{\{3,4,...,p\}}$ such that $\sigma_1 = E_2(\sigma_1, \tau_1)$ and $\sigma_2 = E_2(\sigma_2, \tau_2)$.

If τ_1 is an odd permutation, we replace τ_1 by $\theta_1 = \tau_1(p - 1, p)$. Thus, we have that $\sigma_1 = E_2(\sigma_1, \theta_1)$, with $\theta_1 \in A_p$.

Analogously , if τ_2 is an odd permutation, we replace τ_2 by $\theta_2 = \tau_2(1, 2)$ and we conclude that $\sigma_2 = E_2(\sigma_2, \theta_2)$, with $\theta_2 \in A_p$.

That is, we have found two permutation ζ_1 and ζ_2 in A_p such that

$$\sigma = \sigma_1\sigma_2 = E_2(\sigma_1, \zeta_1)E_2(\sigma_2, \zeta_2).$$ □

Lemma 3.3 solves the problem for permutations of type 1.

Lemma 3.4. *Let σ be a permutation in A_n, $n = supp(\sigma)$, that can be expressed as a product of two or more disjoint 3-cycles. Then σ can be written as product of two Engel words of length two in A_n.*

Proof.

Let $\sigma = \sigma_1...\sigma_r$ be a permutation with $r \geq 2$ and σ_i a 3−cycle for every $i \in \{1, ..., r\}$.

If r is even, we can group the 3-cycles in pairs. It is sufficient to prove the thesis for $r = 2$ and use Corollary 2.1.

So, let's suppose that $\sigma = (a,b,c)(d,e,f)$. Since $(a,b,c) = E_2((a,b,c),(a,b))$ and $(d,e,f) = E_2((d,e,f),(d,e))$, we have that

$$\begin{aligned}\sigma &= E_2((a,b,c),(a,b))E_2((d,e,f),(d,e)) = \\ &= E_2((a,b,c)(d,e,f),(a,b)(d,e)) \in E_2(A_6).\end{aligned}$$

If r is odd (and greater than or equal to 3, by hypothesis) we can group the first three 3-cycles together and the rest of 3-cycles in pairs.

Again, it is sufficient to prove that a product of three 3-cycles can be written as a product of two Engel words of length two in A_9 and use the previous step and Lemma 2.1.

So, let's suppose that $\zeta = (a,b,c)(d,e,f)(g,h,i)$, we have that

$$\zeta = E_2((a,b,c),(a,b))E_2((d,e,f),(d,e))E_2((g,h,i),(g,h)).$$

Applying Lemma 2.1 in the two first Engel words of the last formula, we have that

$$\begin{aligned}\zeta &= E_2((a,b,c)(d,e,f),(a,b)(d,e))E_2((g,h,i),(g,h)) = \\ &= E_2((a,b,c)(d,e,f),(a,b)(d,e))E_2((g,h,i),(a,b)(g,h)) \in E_2(A_n)E_2(A_n).\end{aligned}$$

Even more,

$$\zeta = E_2((a,b,c)(d,e,f)(g,h,i),(a,b)(d,e)(g,h)) \in E_2(S_9) \qquad \square$$

Corollary 3.1. *Let σ be a permutation in A_n, $n = supp(\sigma)$, that can be expressed as a product of an even number of disjoint 3-cycles. Then σ can be written as a single Engel word of length two in A_n.*

If σ is a permutation in A_n, $n = supp(\sigma)$, that can be expressed as a product of cycles of odd length and the number of 3-cycles is not one, then σ is a product of two Engel words in A_n. This follows immediately from Lemmas 3.3 and 3.4 and Corollary 2.1.

It remains to consider the case in which the expression of σ involves only pairs of elements of even length (type 3) or exactly one 3-cycle (type 4).

Lemma 3.5. *Let σ be a permutation in A_n, $n = supp(\sigma)$, that can be expressed as a product of two disjoint cycles of even length, then σ can be written as a product of two Engel words of length two in A_n.*

Proof. Lemma 3.1 solves the case when σ is a product of two transpositions. Let's consider $\sigma = \sigma_1\sigma_2$, with σ_1 and σ_2 cycles of even length. Suppose that $\sigma_1 = (a_1,...,a_r)$ and $\sigma_2 = (b_1,...,b_t)$, where r,t are even.

If $r,t \geq 4$, we can rewrite σ_1 and σ_2 as follows:

$$\begin{aligned}\sigma_1 &= (a_1,...,a_r) = (a_1,...,a_{r-1})(a_{r-1},a_r) = \zeta_1(a_{r-1},a_r); \\ \sigma_2 &= (b_1,...,b_t) = (b_1,...,b_{t-1})(b_{t-1},b_t) = \zeta_2(b_{t-1},b_t).\end{aligned}$$

Applying Lemma 3.2, we know that there exist $\lambda_1 \in S_{p-1}$ and $\lambda_2 \in S_{t-1}$, such that $E_2(\zeta_i, \lambda_i) = \zeta_i$, with $i \in \{1, 2\}$.

If both λ_1, λ_2 are even (resp. both λ_1, λ_2 are odd), we can use Lemma 2.1 to get

$$\zeta_1\zeta_2 = E_2(\zeta_1\zeta_2, \lambda_1\lambda_2) \in E_2(A_n).$$

If λ_1 is even and λ_2 is odd (resp. λ_1 is odd and λ_2 is even), it is sufficient to see that $\zeta_2 = E_2(\zeta_2, \lambda_2(a_r, b_t)) \in E_2(A_n)$. Since ζ_1, λ_1 commute with $\zeta_2, \lambda_2(a_r, b_t)$, because they have disjoint supports, we can use Lemma 2.1 to get that

$$\zeta_1\zeta_2 = E_2(\zeta_1\zeta_2, \lambda_1\lambda_2(a_r, b_t)) \in E_2(A_n).$$

By Lemma 3.1 there exist $\tau, \theta \in A_n$ such that

$$(a_{r-1}, a_r)(b_{t-1}, b_t) = E_2(\tau, \theta) \in E_2(A_n).$$

Since $\sigma = \sigma_1\sigma_2 = \zeta_1\zeta_2(a_{r-1}, a_r)(b_{t-1}, b_t)$, we get that $\sigma \in E_2(A_n)E_2(A_n)$.

It remains to prove our result when $r \geq 4$ and $t = 2$. Then we have $\sigma = \sigma_1(b_1, b_2) = \zeta_1(a_{r-1}, a_r)(b_1, b_2)$. Since $\zeta_1 = E_2(\zeta_1, \lambda_1)$, we have two cases:

If $\lambda_1 \in A_n$, then $E_2(\zeta_1, \lambda_1) \in E_2(A_n)$, and we get that $\sigma \in E_2(A_n)$, because $(a_{r-1}, a_r)(b_1, b_2) \in E_2(A_n)$ by Lemma 3.1.

If $\lambda_1 \in S_n \setminus A_n$, we replace λ_1 by $\beta_1 = \lambda_1(b_1, b_2) \in A_n$. Thus, we have that $\zeta_1 = E_2(\zeta_1, \beta_1) \in E_2(A_n)$ and again, $\sigma \in E_2(A_n)E_2(A_n)$. □

The only case that remains is when σ involves only one 3-cycle.

Lemma 3.6. *Let σ be a permutation in A_n of type 3, $n = supp(\sigma)$. Then σ can be written as a product of two Engel words of length two in A_n.*

Proof. Let σ be a permutation in A_n that can be expressed as $\sigma = \sigma_1\tilde{\sigma_2}\tilde{\sigma_3}$, with σ_1 a 3−cycle, $\tilde{\sigma_2}$ a product of cycles of odd length greater than 3 and $\tilde{\sigma_3}$ a product of an even number of cycles of even length. We will study two different cases:

1. If $\tilde{\sigma_3} = 1$, we consider $\sigma = (a, b, c)\tilde{\sigma_2}$. Any cycle factor τ of $\tilde{\sigma_2}$ has odd length greater than 3, so τ is an Engel word of length two in $S_{supp\tau}$.
   So $\tilde{\sigma_2} = E_2(\tilde{\sigma_2}, \theta)$ is an Engel word of length two in $S_{supp\tilde{\sigma_2}}$.
   By the other side, $\sigma = (a, b, c)\tilde{\sigma_2}$ and $(a, b, c) = E_2((a, b, c), (a, b))$.
   If $\theta \in S_n \setminus A_n$, $\sigma = E_2(\sigma, \theta(a, b)) \in E_2(A_n)$.
   If $\theta \in A_n$, then $\sigma = (a, b, c)\tilde{\sigma_2} = E((a, b, c), (a, b)\theta)E_2(\tilde{\sigma_2}, \theta) \in E_2(A_n)E_2(A_n)$.
2. If $\tilde{\sigma_3} \neq 1$, we know that $(a, b, c)\tilde{\sigma_2} \in E_2(A_n)E_2(A_n)$. Then $(a, b, c)\tilde{\sigma_2} = E_2(\theta_1, \eta_1)E_2(\theta_2, \eta_2)$ and $\tilde{\sigma_3} = E_2(\theta_3, \eta_3)E_2(\theta_4, \eta_4)$ by Lemma 3.5, where $\{\theta_1, \theta_2, \eta_1, \eta_2\}$ are disjoint with $\{\theta_3, \theta_4, \eta_3, \eta_4\}$.
   So $\sigma = (a, b, c)\tilde{\sigma_2}\tilde{\sigma_3}$ can be written as

$$\sigma = E_2(\theta_1, \eta_1)E_2(\theta_2, \eta_2)E_2(\theta_3, \eta_3)E_2(\theta_4, \eta_4),$$

   and applying Lemma 2.1 we get that

$$\sigma = E_2(\theta_1\theta_3, \eta_1\eta_3)E_2(\theta_2\theta_4, \eta_2\eta_4) \in E_2(A_n)E_2(A_n).$$

□

This finishes the proof of Theorem 2.1 for Engel words of length two.

4. The general case

In this section we will extend Theorem 2.1 to Engel words of arbitrary length, proving that every element in the alternating group A_n, can be written as a product of two Engel words of length m in A_n.

First we need to extend Lemma 3.1 to the case of Engel words of arbitrary length.

Lemma 4.1. *Let $\sigma = (1,2)(3,4) \in A_4$. Then for every $m \in \mathbb{N}$, σ is an Engel word of length m in A_n.*

Proof.

$$\begin{array}{lll} (1,2)(3,4) = E_m((1,3,4),(1,2,4)) & \text{if} & m \equiv 0 \mod(3), \\ (1,2)(3,4) = E_m((1,4,3),(1,2,3)) & \text{if} & m \equiv 1 \mod(3), \\ (1,2)(3,4) = E_m((1,4,2),(1,3,4)) & \text{if} & m \equiv 2 \mod(3). \end{array}$$

□

Now, we will extend Lemma 3.2 to Engel words of arbitrary length.

Lemma 4.2. *Let σ be a cycle in A_n of length r odd and greater than or equal to 3. Then, σ can be written as a single Engel word in A_{r+2}.*

Proof. Applying Lemma 3.2, we know that there exist $\tau \in A_{r+2}$ such that $[\sigma, \tau] = \sigma$. Then,

$$E_m(\sigma,\tau) = [...[\sigma, \overbrace{\tau], \tau}^{m}], ..., \tau] = \sigma.$$

□

Remark. As in Lemma 3.2, we also have that $\sigma \in E_m S_r$, that is, there is $\tau' \in S_r$ such that $E_m(\sigma, \tau') = \sigma$ for all $m \in \mathbb{N}$.

Lemma 4.3. *Every cycle σ of odd length $n \geq 5$ can be written as a product of two Engel words of length m in A_n.*

Proof. Let $\sigma = (1, ..., n)$ and rewrite σ as $\sigma_1\sigma_2$ with $\sigma_1 = (1,2,3)$ and $\sigma_2 = (3,4,5,...,n)$. We have seen in Lemma 3.3 that there exist $\zeta_1, \zeta_2 \in A_n$ such that $\sigma_i = E_2(\sigma_i, \zeta_i)$ with $i \in \{1,2\}$. Then $\sigma_i = E_m(\sigma_i, \zeta_i)$ for an arbitrary m and

$$\sigma = E_m(\sigma_1, \zeta_1)E_m(\sigma_2, \zeta_2).$$

□

We can easily extend Lemma 3.4 to Engel words of arbitrary length.

Lemma 4.4. *Let σ be an even permutation in A_n that can be expressed as a product of, at least, two disjoint 3-cycles. Then for every $m \geq 2$, σ can be written as a product of two Engel words of length m in A_n, $n = supp(\sigma)$.*

Proof. As in Lemma 3.4, it is sufficient to prove this Lemma when σ is a product of two or three 3-cycles. In the proof of Lemma 3.4, we got that

$$E_2((a,b,c)(d,e,f),(a,b)(d,e)) = (a,b,c)(d,e,f),$$
$$E_2((g,h,i),(g,h)(a,b)) = (g,h,i).$$

So,

$$(a,b,c)(d,e,f) = E_m((a,b,c)(d,e,f),(a,b)(d,e)),$$
$$(g,h,i) = E_m((g,h,i),(g,h)(a,b)).$$

Corollary 2.1 finishes the proof. □

If σ is a permutation in A_n, $n = supp(\sigma)$, that can be written as a product of cycles of odd length and the number of 3-cycles is not 1 (that is σ is of type 1 or 2), the result holds for σ.

Lemma 4.5. *Let σ be a permutation in A_n, $n = supp(\sigma)$, that can be expressed a product of two disjoint cycles of even length, then for every $m \in \mathbb{N}$, σ can be written as a product of two Engel words of length m in A_n. Consequently the result holds for permutations of type 3.*

Proof. The proof follows the lines of the proof of Lemma 3.5. □

We only need, to finish the proof of Theorem 2.1, consider permutations of type 4.

Lemma 4.6. *Let σ be a permutation of type 4 in A_n. Then for every $m \in \mathbb{N}$, σ can be written as a product of two Engel words of length m in A_n.*

Proof.
The proof repeats the arguments used to prove Lemma 3.6. □

Acknowledgements

This work was partially supported by BES-2011-044790 (research fellowship associated to project MTM2013-45588-C3-1-P) and GRUPIN 14-142.

References

[1] W. J. Ellison, *Warings's Problem.* Amer. Math. Monthly 78 (1971), no. 1, 10–36.
[2] M. Larsen and A. Shalev, *World maps and Waring type problems.* J. Amer. Math. Soc. 22 (2009), no. 2, 437–466.

[3] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep. *The Ore Conjecture*. J. Eur. Math. Soc. (JEMS) 12 (2010), no. 4, 939–1008.
[4] M. W. Liebeck and A. Shalev, *Diameter of simple groups: sharp rounds and applications*. Ann. of Math. (2) 154 (2001), no. 2, 383–406.
[5] M. J. Larsen, A. Shalev and P. H. Tiep, *The Waring problem for finite simple groups*. Ann. of Math. (2) 174 (2011), no. 3, 1885–1950.
[6] C. Martinez and E. I. Zelmanov, *Product of powers in finite simple groups*. Israel J. Math. 96 (1996), part B, 469–479.
[7] O. Ore, *Some Remarks on Commutators*. Proc. Amer. Math. Soc. 2, (1951). 307–314.
[8] J. Saxl and J. S. Wilson, *A note on powers in simple groups*. Math. Proc. Cambridge Philos. Soc. 122 (1997), no. 1, 91–94.
[9] D. Segal, *Words: notes on verbal width in groups*. London Mathematical Society Lecture Note Series, 361. Cambridge University Press, Cambridge, 2009.
[10] J. S. Wilson, *First-order group theory*. Infinite Groups (1994). Gruyter, Berlin, 1996, pp. 301–314.

Apéndice B

Resultados computacionales para cadenas de Engel

Listaremos algunos de los resultados obtenidos computacionalmente, usando los algoritmos descritos en el Capítulo 4, para encontrar las cadenas de Engel en grupos alternados pequeños. Proporcionaremos la lista íntegra de cadenas y bucles en el grupo alternado A_5 para un elemento de cada tipo.

Para los grupos alternados A_6 y A_7, listaremos algunas de las cadenas asociadas a diversos elementos en el grupo que nos han permitido probar el Teorema 4.2.5 para estos grupos.

Se va a dar la lista de las cadenas de longitud máxima asociadas al elemento (1,2,3,4,5) en el grupo alternado de grado 5.

• La cadena que comienza en E_0((),(1,2,3,4,5)) es:
[()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((3,4,5),(1,2,3,4,5)) es:
[(3,4,5), (1,4,3), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4)]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((3,5,4),(1,2,3,4,5)) es:
[(3,5,4), (1,5,3), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4)]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,3)(4,5),(1,2,3,4,5)) es:
[(2,3)(4,5), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3)]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,3,4),(1,2,3,4,5)) es:
[(2,3,4), (2,5,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2)]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,3,5),(1,2,3,4,5)) es:
[(2,3,5), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4)]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,4,3),(1,2,3,4,5)) es:
[(2,4,3), (2,5,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2)]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,4,5),(1,2,3,4,5)) es:
[(2,4,5), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4)]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,4)(3,5),(1,2,3,4,5)) es:

```
[ (2,4)(3,5), (1,4,2), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((2,5)(3,4),(1,2,3,4,5)) es:
[ (2,5)(3,4), (1,3,5,2,4), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2)(4,5),(1,2,3,4,5)) es:
[ (1,2)(4,5), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4) ]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2)(3,4),(1,2,3,4,5)) es:
[ (1,2)(3,4), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2)(3,5),(1,2,3,4,5)) es:
[ (1,2)(3,5), (1,3,5,2,4), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,3),(1,2,3,4,5)) es:
[ (1,2,3), (1,4,2), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,3,4,5),(1,2,3,4,5)) es:
[ (1,2,3,4,5), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,3,5,4),(1,2,3,4,5)) es:
[ (1,2,3,5,4), (2,5,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,4,5,3),(1,2,3,4,5)) es:
[ (1,2,4,5,3), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,4),(1,2,3,4,5)) es:
[ (1,2,4), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2) ]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
```

```
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,4,3,5),(1,2,3,4,5)) es:
[ (1,2,4,3,5), (1,4,3), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4) ]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,5,4,3),(1,2,3,4,5)) es:
[ (1,2,5,4,3), (2,5,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2) ]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,5),(1,2,3,4,5)) es:
[ (1,2,5), (1,5,3), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,2,5,3,4),(1,2,3,4,5)) es:
[ (1,2,5,3,4), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3,2),(1,2,3,4,5)) es:
[ (1,3,2), (1,4,3), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4) ]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3,4,5,2),(1,2,3,4,5)) es:
[ (1,3,4,5,2), (1,4,2), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3)(4,5),(1,2,3,4,5)) es:
[ (1,3)(4,5), (1,3,5,2,4), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3,4),(1,2,3,4,5)) es:
[ (1,3,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3,5),(1,2,3,4,5)) es:
[ (1,3,5), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5
```

• La cadena que comienza en E_0((1,3)(2,4),(1,2,3,4,5)) es:
[(1,3)(2,4), (1,5,3), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4)]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3,2,4,5),(1,2,3,4,5)) es:
[(1,3,2,4,5), (2,5,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2)]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3)(2,5),(1,2,3,4,5)) es:
[(1,3)(2,5), (2,5,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2)]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,3,4,2,5),(1,2,3,4,5)) es:
[(1,3,4,2,5), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4)]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4,5,3,2),(1,2,3,4,5)) es:
[(1,4,5,3,2), (1,5,3), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4)]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4,5),(1,2,3,4,5)) es:
[(1,4,5), (2,5,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2)]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4)(3,5),(1,2,3,4,5)) es:
[(1,4)(3,5), (2,5,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2)]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4,5,2,3),(1,2,3,4,5)) es:
[(1,4,5,2,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2)]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4)(2,3),(1,2,3,4,5)) es:
[(1,4)(2,3), (1,3,5,2,4), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

```
• La cadena que comienza en E_0((1,4,2,3,5),(1,2,3,4,5)) es:
[ (1,4,2,3,5), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4,2,5,3),(1,2,3,4,5)) es:
[ (1,4,2,5,3), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,3,2,5),(1,2,3,4,5)) es:
[ (1,4,3,2,5), (1,4,2), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,4)(2,5),(1,2,3,4,5)) es:
[ (1,4)(2,5), (1,4,3), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
  (1,5,2,4,3), (1,5,3,2,4) ]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5,4,3,2),(1,2,3,4,5)) es:
[ (1,5,4,3,2), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,5,2),(1,2,3,4,5)) es:
[ (1,5,2), (2,5,3), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2) ]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5,3,4,2),(1,2,3,4,5)) es:
[ (1,5,3,4,2), (2,5,4), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5,4),(1,2,3,4,5)) es:
[ (1,5,4), (1,4,2), (1,5,3,2,4), (1,3,2,5,4), (1,3,5,4,2),
  (1,4,3,5,2), (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,5,3,2,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5)(3,4),(1,2,3,4,5)) es:
[ (1,5)(3,4), (1,4,3,5,2), (1,5,2,4,3), (1,5,3,2,4),
  (1,3,2,5,4), (1,3,5,4,2) ]
El bucle de palabras de Engel comienza en: (1,4,3,5,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5,4,2,3),(1,2,3,4,5)) es:
[ (1,5,4,2,3), (1,4,3), (1,3,2,5,4), (1,3,5,4,2), (1,4,3,5,2),
```

```
  (1,5,2,4,3), (1,5,3,2,4) ]
El bucle de palabras de Engel comienza en: (1,3,2,5,4)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5)(2,3),(1,2,3,4,5)) es:
[ (1,5)(2,3), (1,5,2,4,3), (1,5,3,2,4), (1,3,2,5,4),
  (1,3,5,4,2), (1,4,3,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5,2,3,4),(1,2,3,4,5)) es:
[ (1,5,2,3,4), (1,5,3), (1,3,5,4,2), (1,4,3,5,2), (1,5,2,4,3),
  (1,5,3,2,4), (1,3,2,5,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 5

• La cadena que comienza en E_0((1,5)(2,4),(1,2,3,4,5)) es:
[ (1,5)(2,4), (1,3,5,2,4), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1
```

Se va a dar la lista de las cadenas de longitud máxima
asociadas al elemento (1,2,3) en el grupo
alternado de grado 5.

• La cadena que comienza en E_0((),(1,2,3)) es:
[()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((3,4,5),(1,2,3)) es:
[(3,4,5), (1,4,3), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((3,5,4),(1,2,3)) es:
[(3,5,4), (1,5,3), (1,3)(2,5), (1,5)(2,3), (1,2)(3,5)]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,3)(4,5),(1,2,3)) es:
[(2,3)(4,5), (1,3,2), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((2,4,3),(1,2,3)) es:
[(2,4,3), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,4,5),(1,2,3)) es:
[(2,4,5), (2,3,4), (1,4)(2,3), (1,2)(3,4), (1,3)(2,4)]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,4)(3,5),(1,2,3)) es:
[(2,4)(3,5), (1,5,4,2,3), (2,3,5), (1,5)(2,3), (1,2)(3,5),
  (1,3)(2,5)]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,5,3),(1,2,3)) es:
[(2,5,3), (1,3)(2,5), (1,5)(2,3), (1,2)(3,5)]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,5,4),(1,2,3)) es:
[(2,5,4), (2,3,5), (1,5)(2,3), (1,2)(3,5), (1,3)(2,5)]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((2,5)(3,4),(1,2,3)) es:
[(2,5)(3,4), (1,4,5,2,3), (2,3,4), (1,4)(2,3), (1,2)(3,4),

```
  (1,3)(2,4) ]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,2)(4,5),(1,2,3)) es:
[ (1,2)(4,5), (1,3,2), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,3),(1,2,3)) es:
[ (1,2,3), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,4,3,5),(1,2,3)) es:
[ (1,2,4,3,5), (1,2,5,4,3), (1,5,3), (1,3)(2,5), (1,5)(2,3),
  (1,2)(3,5) ]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,2,5,3,4),(1,2,3)) es:
[ (1,2,5,3,4), (1,2,4,5,3), (1,4,3), (1,3)(2,4), (1,4)(2,3),
  (1,2)(3,4) ]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,4,5,2),(1,2,3)) es:
[ (1,3,4,5,2), (2,3,4), (1,4)(2,3), (1,2)(3,4), (1,3)(2,4) ]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,5,4,2),(1,2,3)) es:
[ (1,3,5,4,2), (2,3,5), (1,5)(2,3), (1,2)(3,5), (1,3)(2,5) ]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3)(4,5),(1,2,3)) es:
[ (1,3)(4,5), (1,3,2), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3,4),(1,2,3)) es:
[ (1,3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
El bucle de palabras de Engel comienza en: (1,2)(3,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,5),(1,2,3)) es:
[ (1,3,5), (1,2)(3,5), (1,3)(2,5), (1,5)(2,3) ]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,2,4,5),(1,2,3)) es:
[ (1,3,2,4,5), (1,2,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
El bucle de palabras de Engel comienza en: (1,2)(3,4)
```

La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,5,2,4),(1,2,3)) es:
[(1,3,5,2,4), (1,2,3,5,4), (1,2,5), (1,2)(3,5), (1,3)(2,5),
  (1,5)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,2,5,4),(1,2,3)) es:
[(1,3,2,5,4), (1,2,5), (1,2)(3,5), (1,3)(2,5), (1,5)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,3,4,2,5),(1,2,3)) es:
[(1,3,4,2,5), (1,2,3,4,5), (1,2,4), (1,2)(3,4), (1,3)(2,4),
  (1,4)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,5,3,2),(1,2,3)) es:
[(1,4,5,3,2), (1,4,3), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,2),(1,2,3)) es:
[(1,4,2), (1,4)(2,3), (1,2)(3,4), (1,3)(2,4)]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,3,5,2),(1,2,3)) es:
[(1,4,3,5,2), (1,4,5,2,3), (2,3,4), (1,4)(2,3), (1,2)(3,4),
  (1,3)(2,4)]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,5),(1,2,3)) es:
[(1,4,5), (1,2,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4)(3,5),(1,2,3)) es:
[(1,4)(3,5), (1,2,4,5,3), (1,4,3), (1,3)(2,4), (1,4)(2,3),
  (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,5,2,3),(1,2,3)) es:
[(1,4,5,2,3), (2,3,4), (1,4)(2,3), (1,2)(3,4), (1,3)(2,4)]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,2,3,5),(1,2,3)) es:
[(1,4,2,3,5), (1,2,3,4,5), (1,2,4), (1,2)(3,4), (1,3)(2,4),
  (1,4)(2,3)]

El bucle de palabras de Engel comienza en: (1,2)(3,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,2,5,3),(1,2,3)) es:
[(1,4,2,5,3), (1,5,4,2,3), (2,3,5), (1,5)(2,3), (1,2)(3,5),
  (1,3)(2,5)]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4,3,2,5),(1,2,3)) es:
[(1,4,3,2,5), (1,2,5,4,3), (1,5,3), (1,3)(2,5), (1,5)(2,3),
  (1,2)(3,5)]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4)(2,5),(1,2,3)) es:
[(1,4)(2,5), (1,2,3,5,4), (1,2,5), (1,2)(3,5), (1,3)(2,5),
  (1,5)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,4,3,2),(1,2,3)) es:
[(1,5,4,3,2), (1,5,3), (1,3)(2,5), (1,5)(2,3), (1,2)(3,5)]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,2),(1,2,3)) es:
[(1,5,2), (1,5)(2,3), (1,2)(3,5), (1,3)(2,5)]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,3,4,2),(1,2,3)) es:
[(1,5,3,4,2), (1,5,4,2,3), (2,3,5), (1,5)(2,3), (1,2)(3,5),
  (1,3)(2,5)]
El bucle de palabras de Engel comienza en: (1,5)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,4),(1,2,3)) es:
[(1,5,4), (1,2,5), (1,2)(3,5), (1,3)(2,5), (1,5)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5)(3,4),(1,2,3)) es:
[(1,5)(3,4), (1,2,5,4,3), (1,5,3), (1,3)(2,5), (1,5)(2,3),
  (1,2)(3,5)]
El bucle de palabras de Engel comienza en: (1,3)(2,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,2,3,4),(1,2,3)) es:
[(1,5,2,3,4), (1,2,3,5,4), (1,2,5), (1,2)(3,5), (1,3)(2,5),
  (1,5)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,2,4,3),(1,2,3)) es:
[(1,5,2,4,3), (1,4,5,2,3), (2,3,4), (1,4)(2,3), (1,2)(3,4),
  (1,3)(2,4)]
El bucle de palabras de Engel comienza en: (1,4)(2,3)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5,3,2,4),(1,2,3)) es:
[(1,5,3,2,4), (1,2,4,5,3), (1,4,3), (1,3)(2,4), (1,4)(2,3),
  (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,5)(2,4),(1,2,3)) es:
[(1,5)(2,4), (1,2,3,4,5), (1,2,4), (1,2)(3,4), (1,3)(2,4),
  (1,4)(2,3)]
El bucle de palabras de Engel comienza en: (1,2)(3,4)
La longitud del bucle es: 3

Se va a dar la lista de las cadenas de longitud máxima asociadas al elemento (1,2)(3,4) en el grupo alternado de grado 5.

- Los elementos de las clases de conjugación:
[ConjugacyClass(SymmetricGroup([1 .. 5]), (1,2)(3,4))]
no son palabras de Engel de longitud arbitraria de tipo Em(·,(1,2)(3,4)).

- El número de cadenas de longitud máxima es: 47
- El número de cadenas que se estabilizan en el neutro es: 10

- La cadena que comienza en E_0((),(1,2)(3,4)) es:
[()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

- La cadena que comienza en E_0((2,3)(4,5),(1,2)(3,4)) es:
[(2,3)(4,5), (1,4,3,2,5), (1,2,4,5,3), (1,5,2,3,4),
  (1,3,5,4,2)]
El bucle de palabras de Engel comienza en: (1,4,3,2,5)
La longitud del bucle es: 4

- La cadena que comienza en E_0((2,3,4),(1,2)(3,4)) es:
[(2,3,4), (1,4)(2,3), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

- La cadena que comienza en E_0((2,3,5),(1,2)(3,4)) es:
[(2,3,5), (1,4,5,3,2), (1,3,4,2,5), (1,2,3,5,4), (1,5,2,4,3)]
El bucle de palabras de Engel comienza en: (1,4,5,3,2)
La longitud del bucle es: 4

- La cadena que comienza en E_0((2,4,3),(1,2)(3,4)) es:
[(2,4,3), (1,3)(2,4), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

- La cadena que comienza en E_0((2,4,5),(1,2)(3,4)) es:
[(2,4,5), (1,3,5,4,2), (1,4,3,2,5), (1,2,4,5,3), (1,5,2,3,4)]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 4

- La cadena que comienza en E_0((2,4)(3,5),(1,2)(3,4)) es:
[(2,4)(3,5), (1,3,4,2,5), (1,2,3,5,4), (1,5,2,4,3),
  (1,4,5,3,2)]
El bucle de palabras de Engel comienza en: (1,3,4,2,5)
La longitud del bucle es: 4

- La cadena que comienza en E_0((2,5,3),(1,2)(3,4)) es:
[(2,5,3), (1,5,2,3,4), (1,3,5,4,2), (1,4,3,2,5), (1,2,4,5,3)]

El bucle de palabras de Engel comienza en: (1,5,2,3,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((2,5,4),(1,2)(3,4)) es:
[(2,5,4), (1,5,2,4,3), (1,4,5,3,2), (1,3,4,2,5), (1,2,3,5,4)]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 4

• La cadena que comienza en E_0((2,5)(3,4),(1,2)(3,4)) es:
[(2,5)(3,4), (1,5,2)]
El bucle de palabras de Engel comienza en: (1,5,2)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2)(4,5),(1,2)(3,4)) es:
[(1,2)(4,5), (3,5,4)]
El bucle de palabras de Engel comienza en: (3,5,4)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2)(3,4),(1,2)(3,4)) es:
[(1,2)(3,4), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2)(3,5),(1,2)(3,4)) es:
[(1,2)(3,5), (3,4,5)]
El bucle de palabras de Engel comienza en: (3,4,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,3),(1,2)(3,4)) es:
[(1,2,3), (1,3)(2,4), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,3,4,5),(1,2)(3,4)) es:
[(1,2,3,4,5), (1,2,4,5,3), (1,5,2,3,4), (1,3,5,4,2),
  (1,4,3,2,5)]
El bucle de palabras de Engel comienza en: (1,2,4,5,3)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,2,4),(1,2)(3,4)) es:
[(1,2,4), (1,4)(2,3), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,2,4,3,5),(1,2)(3,4)) es:
[(1,2,4,3,5), (1,2,3,5,4), (1,5,2,4,3), (1,4,5,3,2),
  (1,3,4,2,5)]
El bucle de palabras de Engel comienza en: (1,2,3,5,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,2,5,4,3),(1,2)(3,4)) es:
[(1,2,5,4,3), (1,4,3,2,5), (1,2,4,5,3), (1,5,2,3,4),
  (1,3,5,4,2)]

El bucle de palabras de Engel comienza en: (1,4,3,2,5)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,2,5),(1,2)(3,4)) es:
[(1,2,5), (1,2,5)]
El bucle de palabras de Engel comienza en: (1,2,5)
La longitud del bucle es: 2

• La cadena que comienza en E_0((1,2,5,3,4),(1,2)(3,4)) es:
[(1,2,5,3,4), (1,3,4,2,5), (1,2,3,5,4), (1,5,2,4,3),
  (1,4,5,3,2)]
El bucle de palabras de Engel comienza en: (1,3,4,2,5)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,3,2),(1,2)(3,4)) es:
[(1,3,2), (1,4)(2,3), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3,4,5,2),(1,2)(3,4)) es:
[(1,3,4,5,2), (1,4,5,3,2), (1,3,4,2,5), (1,2,3,5,4),
  (1,5,2,4,3)]
El bucle de palabras de Engel comienza en: (1,4,5,3,2)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,3)(4,5),(1,2)(3,4)) es:
[(1,3)(4,5), (1,5,2,4,3), (1,4,5,3,2), (1,3,4,2,5),
  (1,2,3,5,4)]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,3,4),(1,2)(3,4)) es:
[(1,3,4), (1,3)(2,4), ()]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3,5),(1,2)(3,4)) es:
[(1,3,5), (1,2,4,5,3), (1,5,2,3,4), (1,3,5,4,2), (1,4,3,2,5)]
El bucle de palabras de Engel comienza en: (1,2,4,5,3)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,3,2,4,5),(1,2)(3,4)) es:
[(1,3,2,4,5), (1,2,5)]
El bucle de palabras de Engel comienza en: (1,2,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3,5,2,4),(1,2)(3,4)) es:
[(1,3,5,2,4), (1,5,2)]
El bucle de palabras de Engel comienza en: (1,5,2)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,3)(2,5),(1,2)(3,4)) es:
[(1,3)(2,5), (1,3,5,4,2), (1,4,3,2,5), (1,2,4,5,3),

```
  (1,5,2,3,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,3,2,5,4),(1,2)(3,4)) es:
[ (1,3,2,5,4), (3,5,4) ]
El bucle de palabras de Engel comienza en: (3,5,4)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,2),(1,2)(3,4)) es:
[ (1,4,2), (1,3)(2,4), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,3,5,2),(1,2)(3,4)) es:
[ (1,4,3,5,2), (1,3,5,4,2), (1,4,3,2,5), (1,2,4,5,3),
  (1,5,2,3,4) ]
El bucle de palabras de Engel comienza en: (1,3,5,4,2)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,4,3),(1,2)(3,4)) es:
[ (1,4,3), (1,4)(2,3), () ]
El bucle de palabras de Engel comienza en: ()
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,5),(1,2)(3,4)) es:
[ (1,4,5), (1,2,3,5,4), (1,5,2,4,3), (1,4,5,3,2), (1,3,4,2,5) ]
El bucle de palabras de Engel comienza en: (1,2,3,5,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,4)(3,5),(1,2)(3,4)) es:
[ (1,4)(3,5), (1,5,2,3,4), (1,3,5,4,2), (1,4,3,2,5),
  (1,2,4,5,3) ]
El bucle de palabras de Engel comienza en: (1,5,2,3,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,4,5,2,3),(1,2)(3,4)) es:
[ (1,4,5,2,3), (1,5,2) ]
El bucle de palabras de Engel comienza en: (1,5,2)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,2,3,5),(1,2)(3,4)) es:
[ (1,4,2,3,5), (1,2,5) ]
El bucle de palabras de Engel comienza en: (1,2,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4,2,5,3),(1,2)(3,4)) es:
[ (1,4,2,5,3), (3,4,5) ]
El bucle de palabras de Engel comienza en: (3,4,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,4)(2,5),(1,2)(3,4)) es:
[ (1,4)(2,5), (1,4,5,3,2), (1,3,4,2,5), (1,2,3,5,4),
```

```
  (1,5,2,4,3) ]
El bucle de palabras de Engel comienza en: (1,4,5,3,2)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5,4,3,2),(1,2)(3,4)) es:
[ (1,5,4,3,2), (1,5,2,4,3), (1,4,5,3,2), (1,3,4,2,5),
  (1,2,3,5,4) ]
El bucle de palabras de Engel comienza en: (1,5,2,4,3)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5,3,4,2),(1,2)(3,4)) es:
[ (1,5,3,4,2), (1,5,2,3,4), (1,3,5,4,2), (1,4,3,2,5),
  (1,2,4,5,3) ]
El bucle de palabras de Engel comienza en: (1,5,2,3,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5,3),(1,2)(3,4)) es:
[ (1,5,3), (1,3,4,2,5), (1,2,3,5,4), (1,5,2,4,3), (1,4,5,3,2) ]
El bucle de palabras de Engel comienza en: (1,3,4,2,5)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5,4),(1,2)(3,4)) es:
[ (1,5,4), (1,4,3,2,5), (1,2,4,5,3), (1,5,2,3,4), (1,3,5,4,2) ]
El bucle de palabras de Engel comienza en: (1,4,3,2,5)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5)(3,4),(1,2)(3,4)) es:
[ (1,5)(3,4), (1,2,5) ]
El bucle de palabras de Engel comienza en: (1,2,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,5,4,2,3),(1,2)(3,4)) es:
[ (1,5,4,2,3), (3,5,4) ]
El bucle de palabras de Engel comienza en: (3,5,4)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,5)(2,3),(1,2)(3,4)) es:
[ (1,5)(2,3), (1,2,3,5,4), (1,5,2,4,3), (1,4,5,3,2),
  (1,3,4,2,5) ]
El bucle de palabras de Engel comienza en: (1,2,3,5,4)
La longitud del bucle es: 4

• La cadena que comienza en E_0((1,5,3,2,4),(1,2)(3,4)) es:
[ (1,5,3,2,4), (3,4,5) ]
El bucle de palabras de Engel comienza en: (3,4,5)
La longitud del bucle es: 1

• La cadena que comienza en E_0((1,5)(2,4),(1,2)(3,4)) es:
[ (1,5)(2,4), (1,2,4,5,3), (1,5,2,3,4), (1,3,5,4,2),
  (1,4,3,2,5) ]
El bucle de palabras de Engel comienza en: (1,2,4,5,3)
La longitud del bucle es: 4
```

Para el grupo alternado de grado 6, listaremos unas pocas cadenas de modo que en los bucles contenidos en dichas cadenas encontremos un elemento de cada tipo.

• La cadena que comienza en E_0((4,5,6),(1,2,3,4,5)) es:
[(4,5,6), (1,6)(4,5), (1,2,6,5,4), (1,4,2,5)(3,6),
  (1,3,4,2,6), (1,2,5,3)(4,6), (2,4,5,3,6), (1,4,2,3)(5,6),
  (1,4,6,3,5), (1,6)(2,5,3,4), (1,2,5,6,4), (1,4,5,3)(2,6),
  (1,6,5,2,3)]

El bucle de palabras de Engel comienza en: (1,4,2,5)(3,6)
La longitud del bucle es: 10

• La cadena que comienza en E_0((4,5,6),(1,2)(3,4,5,6)) es:
[(4,5,6), (3,5,4), (3,6,5)]

El bucle de palabras de Engel comienza en: (3,5,4)
La longitud del bucle es: 2

 La cadena que comienza en E_0((3,4,5),(1,2,3)(4,5,6)) es:
[(3,4,5), (1,5,4,3,6), (1,5,4)(2,6,3), (2,4)(3,5),
  (1,6)(2,4), (1,6)(3,5)]

El bucle de palabras de Engel comienza en: (2,4)(3,5)
La longitud del bucle es: 3

• La cadena que comienza en E_0((1,4)(2,5,3,6),(1,2)
(3,4)) es:
[(1,4)(2,5,3,6), (1,6,2)(3,4,5)]

El bucle de palabras de Engel comienza en: (1,6,2)(3,4,5)
La longitud del bucle es: 1

Para el grupo alternado de grado 7, listaremos sendas cadenas de modo que en los bucles contenidos en dichas cadenas encontremos un elemento de cada tipo.

• La cadena que comienza en E_0((5,6,7),(1,2,3,4,5,6,7)) es:
[(5,6,7), (1,6,5), (1,5,2,7,6), (1,3)(2,5,7,6),
  (1,6,3,7,5,4,2), (1,7,2)(3,5,4), (2,7,3,6,5),
  (1,4,7,2,5,3,6), (1,4,3), (1,3,2,5,4), (1,3)(2,6,5,4),
  (1,7,6,4,3), (1,3,2)(4,6,5), (1,4,7,6,3), (1,3,6,4,7,2,5),
  (2,5,4), (2,4,3,6,5), (2,4)(3,7,6,5), (1,7,5,4,2),
  (2,4,3)(5,7,6), (1,7,4,2,5), (1,3,6,2,4,7,5), (3,6,5),
  (3,5,4,7,6), (1,7,6,4)(3,5), (1,6,5,3,2), (1,7,6)(3,5,4),
  (1,5,3,6,2), (1,6,2,4,7,3,5), (4,7,6), (1,7,4,6,5),
  (1,7,5,2)(4,6), (2,7,6,4,3), (1,7,2)(4,6,5), (2,6,4,7,3),
  (1,4,6,2,7,3,5), (1,7,5), (1,5,7,6,2), (1,6,3,2)(5,7),
  (1,7,5,4,3), (1,3,2)(5,7,6), (1,4,3,7,5), (1,4,6,2,5,7,3),
  (1,6,2), (1,7,3,2,6), (1,6)(2,7,4,3), (1,6,5,4,2),
  (1,7,6)(2,4,3), (1,6,2,5,4), (1,4,2,5,7,3,6), (2,7,3),
  (1,4,3,7,2), (1,5,4,3)(2,7), (2,7,6,5,3)]
El bucle de palabras de Engel comienza en: (1,7,2)(3,5,4)
La longitud del bucle es: 49

• La cadena que comienza en E_0((3,4)(6,7),(1,2,3)) es:
[(3,4)(6,7), (1,4,3), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4)]
El bucle de palabras de Engel comienza en: (1,3)(2,4)
La longitud del bucle es: 3